Action Refinement in Conformance Testing

Machiel van der Bijl* and Arend Rensink
Software Engineering, Department of Computer Science,
University of Twente
P.O. Box 217, 7500 AE Enschede, The Netherlands
email: {vdbijl, rensink}@cs.utwente.nl

Jan Tretmans
Nijmegen Institute for Computing and Information Sciences
Radboud University Nijmegen
P.O. Box 9010 6500 GL Nijmegen The Netherlands
email: tretmans@cs.kun.nl

Abstract

In *model based testing* test cases are derived from a model (the specification) of the system we want to test. In general the model is more abstract than the implementation. This may result in test cases that are not executable, because their actions are too abstract; the implementation does not understand them. The standard approach is to rewrite the model by hand to the required level of detail and regenerate the test cases. This is error-prone and time consuming.

In this paper we present an approach to automatically obtain test cases at the required level of detail by means of action refinement. Action refinement is a way to add information to the abstract model. It relates actions from the abstract model to concrete actions of the system under test. We apply this approach to a simple case of action refinement, so-called atomic linear input-inputs refinement. In order to reason about correctness between an abstract model and a concrete implementation we introduce a new implementation relation. We show that this relation is equivalent with the **uioco** implementation relation on the refined model. Furthermore we show under which conditions the refinement of a complete abstract test suite is again complete.

1 Introduction

A problem in model based testing is that the generated test cases do not have the required level of abstraction, and hence are not executable against the implementation under test. This problem arises because the test cases are generated

*This research was supported by the dutch research program PROGRESS under project: TES5417: Atomyste – ATOm splitting in eMbedded sYStems TEsting.

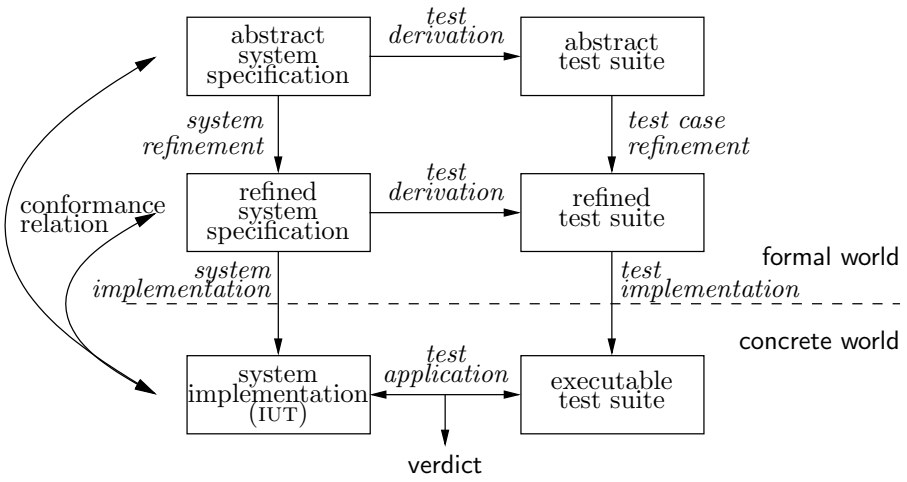

Figure 1: Action refinement approach

from the model and in general, the model is more abstract than the implementation. The usual solution is to add the required level of detail to the model by hand. This has some obvious drawbacks; it is time consuming and error-prone.

In this paper we use *action refinement* to automatically obtain test cases at the required level of detail. Action refinement has been studied extensively; see Gorrieri and Rensink for an overview [2]. Action refinement adds extra information to the model by relating an action of the model to more detailed behavior. Wherever we read the action in the model we replace it with the more detailed behavior. For example, if the model tells us to input two euros and the implementation also allows the insertion of two one euro pieces, with action refinement we can define that wherever we read two euros we can also read the more detailed behavior one euro followed by one euro.

Action refinement in model based testing has not been studied at all. This is surprising, because it is a well known problem in practice and occurs often.

Figure 1 shows our general approach for action refinement in testing. We see six objects in the figure. The objects on the left hand side denote models and the objects on the right hand side denote test suites. **System implementation** is the system that we want to test, also known as IUT (Implementation Under Test); a real system in the physical world. **Abstract system specification** is a (formal) model of the system implementation. It is called *abstract* because it does not have the required level of detail with respect to the system implementation. **Refined system specification** is the refined model of the system implementation with the required level of abstraction with respect to the system implementation. **Abstract test suite** is the test suite that is derived from the abstract system specification. As with the abstract system specification, it is too abstract with respect to the system implementation. **Refined test suite** is a test suite with the required level of abstraction with respect to the system implementation. There are two ways to derive such a test suite. One way is to refine the abstract test suite, another way is to derive test cases from the refined system specification. We do both and proof both approaches to be equivalent under certain restrictions. **Executable test suite** is a test suite in the physical

world that we can execute against the system implementation. This results in a verdict whether or not the implementation is correct with respect to the refined (or abstract) system specification. This notion of correctness is defined in a so-called *implementation relation* between the system specification (abstract or refined) and the system implementation. The conformance relation is depicted on the left side of the Figure.

This paper is a first step in our effort towards action refinement in model based testing and we use a simple, though non-trivial case of action refinement: *atomic linear input-inputs refinement*.

In this paper we show how to refine traces, transition systems and test cases. In order to reason about correctness between an abstract specification and a concrete implementation we introduce the implementation relation $\mathbf{uioco}_r$ and we show that it is equivalent with **uioco** between the refined specification and the same implementation (**uioco** is a further evolution of **ioco**; see [5] and [8]). We show under which conditions the refinement of a complete abstract test suite results in a complete refined test suite.

The main contribution of this paper is that refinement of a complete test suite results in a complete refined test suite (under certain restrictions). Furthermore we argue that the approach that we use for atomic linear input-inputs refinement can be extended to more general types of action refinement. This extension is the next step in our research. One of the surprising (theoretic) consequences of this paper is the fact that specification equivalence is not preserved by action refinement.

We start with summarizing some results and notations that we will use throughout the paper in Section 2. In Section 3 we introduce atomic linear input-inputs refinement. We present trace refinement in Section 4 and the refinement of labeled transition systems in Section 5. In Section 6 we present the implementation relation $\mathbf{uioco}_r$, followed by the refinement of test cases in Section 7. Conclusions can be found in Section 8.

2 Formal preliminaries

This section recalls some aspects of the theory behind **uioco** that are used in this paper; see [8] and [5] for a more detailed exposition.

Labeled Transition Systems. A labeled transition system (LTS) description is defined in terms of states and labeled transitions between states, where the labels indicate what happens during the transition. Labels are taken from a global set $\mathbf{L}$. We use a special label $\tau \notin \mathbf{L}$ to denote an internal action. For arbitrary $L \subseteq \mathbf{L}$, we use L_τ as a shorthand for $L \cup \{\tau\}$. We partition the label set of an LTS in an input and output set; a deviation from the standard definition of labeled transition systems.

Definition 2.1 A *labeled transition system* is a 5-tuple $\langle Q, I, U, T, q_0 \rangle$ where Q is a non-empty countable set of *states*; $I \subseteq \mathbf{L}$ is the countable set of *input labels*; $U \subseteq \mathbf{L}$ is the countable set of *output labels*, $I \cap U = \emptyset$; $T \subseteq Q \times (I \cup U \cup \{\tau\}) \times Q$ is a set of triples, the *transition relation*; $q_0 \in Q$ is the *initial state*.

We use L as shorthand for the entire label set ($L = I \cup U$); furthermore, we use Q_p, I_p, etc. to denote the components of an LTS p. We commonly write

$q \xrightarrow{\mu} q'$ for $(q, \mu, q') \in T$. We use a question mark before a label to denote that it is an input action (i.e., an element of I) and an exclamation mark to denote that it is an output action (i.e., an element of U). We denote the class of all labeled transition systems over I and U by $\mathcal{LTS}(I, U)$. We represent a labeled transition system in the standard way, by a directed, edge-labeled graph where nodes represent states and edges represent transitions.

A state that cannot do an internal action is called *stable*. A stable state from which no output action is possible is called *quiescent*. We use the symbol δ ($\notin \mathbf{L}_\tau$) to represent quiescence: $p \xrightarrow{\delta} p$ stands for the absence of any transition $p \xrightarrow{\mu} p'$ with $\mu \in U_\tau$. For an arbitrary $L \subseteq \mathbf{L}$, we use L_δ as a shorthand for $L \cup \{\delta\}$. We use the label μ, respectively λ, to range over $\mathbf{L}_\tau$, respectively $\mathbf{L}_{\tau\delta}$.

An LTS is *strongly responsive* if it always eventually enters a quiescent state; in other words, if it does not have infinite U_τ-labeled paths. The **ioco** theory is restricted to strongly responsive systems. We also use this restriction because we reuse results of the **ioco** theory.

A *trace* is a sequence of observable actions. The set of all traces over L ($\subseteq \mathbf{L}$) is denoted by L^*, ranged over by σ, with ϵ denoting the empty sequence. If $\sigma_1, \sigma_2 \in L^*$, then $\sigma_1 \cdot \sigma_2$ is the concatenation of σ_1 and σ_2. Concatenation is extended in the standard way to sets of traces and also to $\Sigma \cdot a$ where Σ is a set of traces and a an action. We use the standard notation with single and double arrows for traces: $q \xrightarrow{\lambda_1 \cdots \lambda_n} q$ denotes $q \xrightarrow{\lambda_1} \cdots \xrightarrow{\lambda_n} q'$, $q \overset{\epsilon}{\Longrightarrow} q'$ denotes $q \xrightarrow{\tau \cdots \tau} q'$ and $q \overset{\lambda_1 \cdots \lambda_n}{\Longrightarrow} q$ denotes $q \overset{\epsilon}{\Longrightarrow} \xrightarrow{\lambda_1} \overset{\epsilon}{\Longrightarrow} \cdots \xrightarrow{\lambda_n} \overset{\epsilon}{\Longrightarrow} q'$. We will use Σ to denote a set of traces. If $\sigma = \lambda_1 \cdots \lambda_n$ then $\sigma | i = \lambda_i$ for $1 \leq i \leq |\sigma| = n$, and $L(\sigma) = \{\lambda_1, \cdots, \lambda_n\}$. We use the symbol $\sqsubseteq$ to denote trace prefix and the symbol $\downarrow$ to denote prefix closure, as follows: $\sigma_1 \sqsubseteq \sigma \Leftrightarrow \exists \sigma_2 : \sigma_1 \cdot \sigma_2 = \sigma$, $\downarrow \sigma = \{\sigma' \mid \sigma' \sqsubseteq \sigma\}$, $\downarrow \Sigma = \bigcup \{\downarrow \sigma \mid \sigma \in \Sigma\}$

We will not always distinguish between a labeled transition system and its initial state. We will identify the process $p = \langle Q, I, U, T, q_0 \rangle$ with its initial state q_0, and we write, for example, $p \overset{\sigma}{\Longrightarrow} q_1$ instead of $q_0 \overset{\sigma}{\Longrightarrow} q_1$.

Input-output transition systems. We call a labeled transition system that is completely specified for input actions an *input-output transition system* (IOTS). This means that all states can do all input actions from the label set, if necessary by first doing one or more internal actions.

Definition 2.2 An *input-output transition system* $p = \langle Q, I, U, T, q_0 \rangle$ is a labeled transition system for which all inputs are enabled in all states: $\forall q \in Q, a \in I : q \overset{a}{\Longrightarrow}$ (*weak* input enabledness).

The class of input-output transition systems with input actions in I and output actions in U is denoted by $\mathcal{IOTS}(I, U)$ ($\subseteq \mathcal{LTS}(I, U)$).

Conformance. The testing scenario on which **uioco** is based wants to establish a notion of conformance between a specification and an implementation [5]. The specification is an LTS, specifying the required behavior. Since the testing approach is black box testing, we do not know anything about the implementation; however, we *assume* that it is possible to model it as an IOTS. This assumption is referred to as the test hypothesis [1].

Given a specification s and an (assumed) model of the implementation i, the relation i **ioco**$_\mathcal{F}$ s expresses that i conforms to s based on a set of traces $\mathcal{F}(s)$.

This is formalized as follows (where $s \in \mathcal{LTS}(I,U)$, $i \in \mathcal{IOTS}(I,U)$, $S \subseteq Q_s$ be a set of states in s, $\sigma \in \mathbf{L}_\delta^*$ and $\mathcal{F} : \mathcal{LTS}(I,U) \to 2^{L_\delta^*}$).

$$
\begin{aligned}
s \textbf{ after } \sigma &=_{\text{def}} \{s' \mid s \stackrel{\sigma}{\Longrightarrow} s'\} && (1)\\
out(s) &=_{\text{def}} \{x \in U \mid s \stackrel{x}{\longrightarrow}\} \cup \{\delta \mid s \stackrel{\delta}{\longrightarrow}\} && (2)\\
out(S) &=_{\text{def}} \bigcup\{out(s) \mid s \in S\} && (3)\\
Straces(s) &=_{\text{def}} \{\sigma \in L_\delta^* \mid s \stackrel{\sigma}{\Longrightarrow}\} && (4)\\
Utraces(s) &=_{\text{def}} \{\sigma \in Straces(s) \mid \forall q, (\sigma_1 \cdot a) \sqsubseteq \sigma : \\
&\qquad (a \in I \wedge s \stackrel{\sigma_1}{\Longrightarrow} q) \Rightarrow q \stackrel{a}{\Longrightarrow}\} && (5)\\
i \textbf{ ioco}_{\mathcal{F}}\ s &=_{\text{def}} \forall \sigma \in \mathcal{F}(s) : out(i \textbf{ after } \sigma) \subseteq out(s \textbf{ after } \sigma) && (6)
\end{aligned}
$$

For $\mathcal{F}(s) = Straces(s)$ we abbreviate $\textbf{ioco}_{\mathcal{F}}$ to **ioco**; for $\mathcal{F}(s) = Utraces(s)$ we abbreviate it to **uioco**. In other words **ioco** is based on suspension traces (*Straces*: traces in L_δ^*) whereas **uioco** is based on a subset of suspension traces: universal traces. All states that a universal trace leads to can do the same set of input actions. This is a necessary prerequisite to use **uioco** for compositional testing (see [8]).

Test cases. A test case is the specification of a tester in an experiment with the system under test. It is modeled as a special labeled transition system with **pass** and **fail** predicates on states to decide about the success of a test. It is a special LTS because it has the following restrictions:

Definition 2.3 A test case $t = \langle Q, S, R, T, t_0, \textbf{pass}, \textbf{fail}\rangle$ over a set of stimuli S and a set of responses R is an acyclic labeled transition system such that:
∘ t is deterministic and has finite behavior.
∘ $\textbf{pass} \subseteq Q, \textbf{fail} \subseteq Q$. **pass** and **fail** states do not have outgoing transitions.
∘ A state in Q that is no **pass** or **fail** state has either *one* outgoing transition with a stimulus label, or has outgoing transitions for *all* labels in R.

The class of test cases over S and R is denoted as $\mathcal{TEST}(S,R)$. A *test suite* T is a set of test cases: $T \subseteq \mathcal{TEST}(S,R)$. An implementation $i \in \mathcal{IOTS}(I,U)$ **passes** a test case $t \in \mathcal{TEST}(I,U_\delta)$ if there is no suspension trace of i that leads to a **fail** state in t. Note that a stimulus of the test case is an input of the implementation and vice versa for the responses. We will use the question and exclamation marks accordingly. See Figure 3 for an example.

Definition 2.4 Let $s \in \mathcal{LTS}(I,U)$ be a specification and $T \subseteq \mathcal{TEST}(I,U_\delta)$ a test suite:
T is **complete** w.r.t. $\textbf{ioco}_{\mathcal{F}}, s \ =_{\text{def}} \forall i \in \mathcal{IOTS}(I,U) : i \textbf{ ioco}_{\mathcal{F}}\ s \Leftrightarrow i \textbf{ passes } T$
T is **sound** w.r.t. $\textbf{ioco}_{\mathcal{F}}, s \ =_{\text{def}} \forall i \in \mathcal{IOTS}(I,U) : i \textbf{ ioco}_{\mathcal{F}}\ s \Rightarrow i \textbf{ passes } T$
T is **exhaustive** w.r.t. $\textbf{ioco}_{\mathcal{F}}, s =_{\text{def}} \forall i \in \mathcal{IOTS}(I,U) : i \textbf{ ioco}_{\mathcal{F}}\ s \Leftarrow i \textbf{ passes } T$

3 Atomic input-inputs action refinement

As stated in the introduction, in this paper we treat the problem that test cases that are derived from a specification may not be executable on the system under test. To illustrate this we start with an example of this problem (we will use this as our running example).

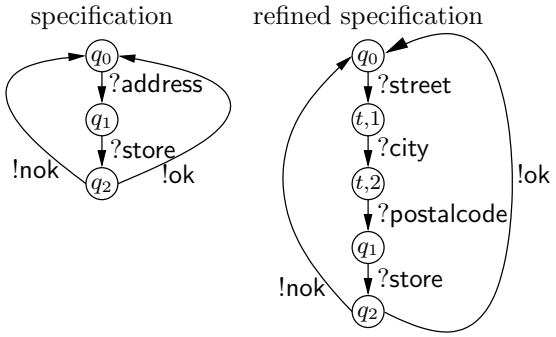

Figure 2: Abstract and refined specification of data entry system

Example 3.1 Figure 2 shows a specification (left) and a refined specification (right) of a very simple data entry application (ignore the state labels for now). The specification tells us that we can enter address data, push the store button and then the system either stores the address data or gives an error. At a certain moment we find out that our specification is too abstract, because an address is entered in three steps instead of one: street, city and postal code. So it behaves more like the refined specification on the right.

The left hand side of Figure 3 shows a test case generated from the abstract specification. On the right we see two test cases with the level of detail that we want to have to test the actual system. We can read the abstract test case as follows: we enter the address data, press the store button and then observe the response of the IUT. The IUT passes the test if we observe ok or nok, but fails if we observe quiescence. □

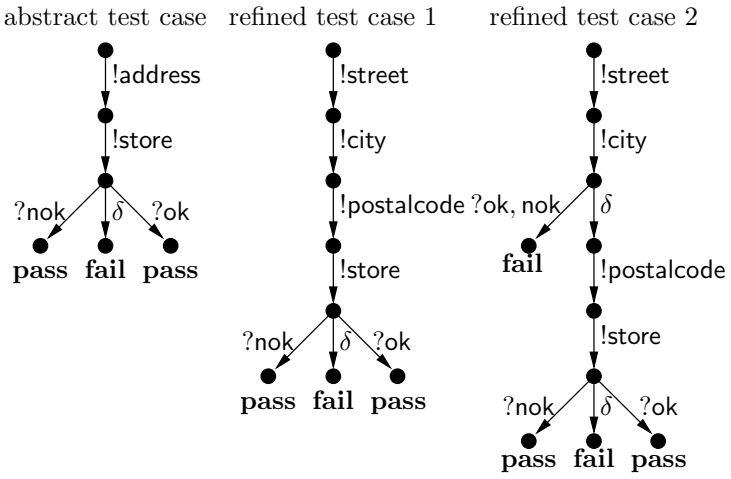

Figure 3: Abstract and refined test cases for data entry example

Of course the data entry example is very simple, because of its educational purposes. This may give the illusion that refinement of transition systems and test cases is straightforward. Our next example illustrates that simple refinements may quickly result in a complex system.

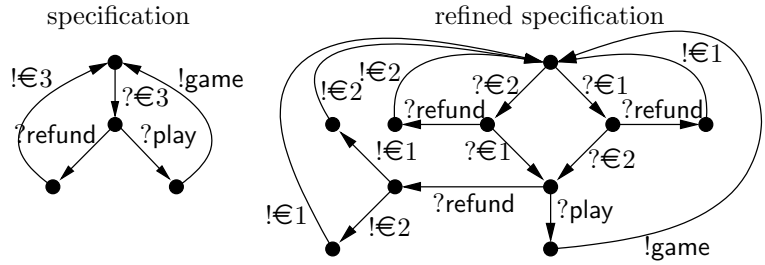

Figure 4: More complicated action refinement example

Example 3.2 In Figure 4, we see the abstract specification (left) and the refined specification (right) of a video game machine. The abstract specification tells us to insert €3 and either press the "play" button to play a video game or press the "refund" button to get the money back. The refined specification is obtained after the two refinements shown in Figure 5 ('E' labels the end state). One refinement is that the €3 input action is refined to €2 followed by €1 or vice versa. In between the coins we can press the "refund" button to get the money back. Likewise the €3 output after pushing the "refund" button is in terms of €1 and €2 coins. To keep the figure readable we left out the refinements for other coins. □

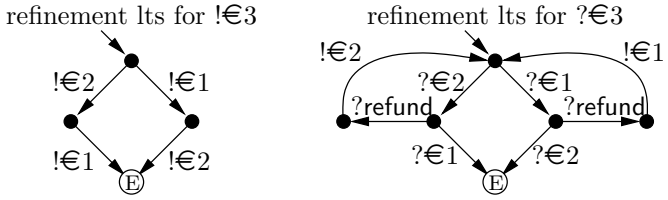

Figure 5: Refinements for the video game example

There are several types of action refinement [7]. In this paper we treat *atomic linear input-inputs refinement*. Atomic means that no actions are allowed to interfere with the refinement; we treat the behavior of the refinement as atomic. Linear means that we allow no branching behavior in the refinement and input-inputs means that we only refine an input action with one or more other input actions. The refinement in Figure 2 is an example of such a refinement, but the refinement in Figure 4 is not. It is our goal to extend this action refinement approach in the future to more general cases of action refinement. We believe that this can be done in a way very similar to the atomic linear input-inputs refinement case that we treat in this paper, as we will discuss in the concluding section.

In this paper we show what correctness means in terms of a conformance relation between the abstract system specification and the system implementation. Furthermore we show two ways to obtain a refined test suite as shown in Figure 1. One is to refine the abstract system specification and derive a refined test suite and the other is to refine the abstract test suite directly. We show that both approaches are equivalent under some restrictions.

Sometimes we use the terms abstract and concrete as synonyms for unrefined and refined, respectively .

4 Trace refinement

We define refinement as a pair $r = (a_r, \sigma_r)$ with respect to an input label set I and an output label set U. a_r is the *refinement label*, i.e., the abstract label that we want to refine and σ_r is the *refinement trace*, i.e., the trace that we want to replace the refinement label with. There are the following restrictions: $a_r \in I$, $L(\sigma_r) \cap L_\delta = \emptyset$ (the labels in σ_r are fresh) and $\sigma_r \neq \epsilon$.

In cases where there may be confusion about label sets we use the subscript r to tag the label set after refinement, for example: $I_r = (I \backslash \{a_r\}) \cup L(\sigma_r)$.

The goal of trace refinement is to refine a trace from an abstract specification such that it becomes a trace of the refined system. In a refined trace all occurrences of the refinement label have been replaced with its refinement.

Input-inputs refinement allows quiescence within a refinement. To get all possible suspension traces within the refinement trace, we saturate the refinement trace with δ's (this technicality is explained in Example 4.4).

Definition 4.1 [δ-saturation] Let $\sigma = a_1 \cdots a_n$ then $\lceil \sigma \rceil = a_1 \cdot \delta^* \cdot a_2 \cdots \delta^* \cdot a_n$

The refinement of a trace results in a set of traces. All labels except the refinement label a_r are unchanged. The refinement label is substituted with every trace in $\lceil \sigma_r \rceil$. Formally this is expressed as follows.

Definition 4.2 [Trace refinement] Let $\sigma \in L_\delta^*$ then $\sigma[r]$ denotes the refinement of a trace in the following way.

$$\sigma[r] = \begin{cases} 1)\ \{\epsilon\} & \text{if } \sigma = \epsilon \\ 2)\ \{\sigma_2 \cdot \lambda \mid \sigma_2 \in \sigma_1[r]\} & \text{if } \sigma = \sigma_1 \cdot \lambda \wedge \lambda \in L_\delta \backslash \{a_r\} \\ 3)\ \{\sigma_2 \cdot \sigma' \mid \sigma_2 \in \sigma_1[r] \wedge \sigma' \in \lceil \sigma_r \rceil\} & \text{if } \sigma = \sigma_1 \cdot a_r \end{cases}$$

Likewise we define refinement on sets of traces by refining all traces in the set.

An important concept in this paper is the concept of an *r-complete* trace. This is a trace that does not end in the middle of a refinement; or in other words, a trace σ is r-complete when $\sigma \in L_\delta^*[r]$.

Trace *contraction* is the opposite of trace refinement. The goal of trace contraction is to transform a concrete trace to a trace of the abstract system.

Definition 4.3 [Trace contraction] Let $r = (a_r, \sigma_r), \sigma \in \downarrow(L_\delta^*[r])$.

$$\sigma\langle r \rangle = \begin{cases} 1)\ \epsilon & \text{if } \sigma = \epsilon \\ 2)\ \sigma_1\langle r \rangle \cdot a_r & \text{if } \sigma = \sigma_1 \cdot \sigma_2 \wedge \sigma_2 \in \lceil \sigma_r \rceil \\ 3)\ \sigma_1\langle r \rangle & \text{if } \sigma = \sigma_1 \cdot \sigma_2 \wedge \sigma_2 \in \downarrow\lceil \sigma_r \rceil \backslash (\lceil \sigma_r \rceil \cup \{\epsilon\}) \\ 4)\ \sigma_1\langle r \rangle \cdot \lambda & \text{if } \sigma = \sigma_1 \cdot \lambda \text{ and none of the above holds} \end{cases}$$

Likewise we define contraction on sets of traces by contracting traces in the set.

Example 4.4 Let us illustrate trace refinement and trace contraction with our running example in Figure 2. We refine the action address into street followed by city followed by postalcode: $r = (\mathsf{address}, \mathsf{street} \cdot \mathsf{city} \cdot \mathsf{postalcode})$. Suppose we

want to refine the trace address·store·ok. This results in the following set of traces of the refined specification.

$$\begin{aligned}(\mathsf{address{\cdot}store{\cdot}ok})[r] &= (\mathsf{address{\cdot}store})[r]{\cdot}\mathsf{ok} && \text{(rule 2)}\\ &= \mathsf{address}[r]{\cdot}\mathsf{store{\cdot}ok} && \text{(rule 2)}\\ &= \mathsf{street}{\cdot}\delta^*{\cdot}\mathsf{city}{\cdot}\delta^*{\cdot}\mathsf{postalcode{\cdot}store{\cdot}ok} && \text{(rule 3)}\end{aligned}$$

To contract $\mathsf{street}{\cdot}\delta{\cdot}\mathsf{city}{\cdot}\mathsf{postalcode{\cdot}store{\cdot}ok}{\cdot}\mathsf{street}{\cdot}\delta$, we obtain the following:

$$\begin{aligned}&(\mathsf{street}{\cdot}\delta{\cdot}\mathsf{city}{\cdot}\mathsf{postalcode{\cdot}store{\cdot}ok}{\cdot}\mathsf{street}{\cdot}\delta)\langle r\rangle\\ &\quad= (\mathsf{street}{\cdot}\delta{\cdot}\mathsf{city}{\cdot}\mathsf{postalcode{\cdot}store{\cdot}ok})\langle r\rangle && \text{(rule 3)}\\ &\quad= (\mathsf{street}{\cdot}\delta{\cdot}\mathsf{city}{\cdot}\mathsf{postalcode{\cdot}store})\langle r\rangle{\cdot}\mathsf{ok} && \text{(rule 4)}\\ &\quad= (\mathsf{street}{\cdot}\delta{\cdot}\mathsf{city}{\cdot}\mathsf{postalcode})\langle r\rangle{\cdot}\mathsf{store{\cdot}ok} && \text{(rule 4)}\\ &\quad= \mathsf{address{\cdot}store{\cdot}ok} && \text{(rule 2)}\end{aligned}$$

□

5 Atomic refinement of transition systems

In this section we present a way to refine transition systems. The crux of this refinement is that we make a transition system from our refinement trace and insert this into the abstract transition system at the place where there is a transition with the abstract refinement label. A formal definition is given in Definition 5.1, it is illustrated in Example 5.2.

Definition 5.1 [Atomic transition system refinement] Let $r = (a_r, \sigma_r)$ be the refinement pair and let $p = \langle Q, I, U, T, q_0\rangle$ be an LTS. We define the refinement of p as $p[r] = \langle Q_r, I_r, U_r, T_r, q_0\rangle$. For a transition $t = (q, a_r, q')$, we use $(t, 0) = q$ and $(t, n) = q'$ for $n = |\sigma_r|$ (this is a technicality to enable refinements of one action).

$Q_r = Q \cup \{(t, i) \mid \exists q, q' \in Q : t = (q, a_r, q') \in T, 1 \leq i < n = |\sigma_r|\}$
$I_r = I \backslash \{a_r\} \cup I(\sigma_r)$
$T' = \{((t, i), \sigma_r|_{i+1}, (t, i + 1)) \mid \exists q, q' \in Q : t = (q, a_r, q') \in T, 0 \leq i < n = |\sigma_r|\}$
$T_r = \{(q, a, q') \in T \mid a \neq a_r\} \cup T'$

To prevent confusion between transitions in the abstract and refined transition system we add the subscript 'r' to the transition arrow for refined systems: $q \overset{\sigma}{\Longrightarrow}_r q'$. Likewise we use the subscript for the set of states, transitions, etc., as shown in the definition.

Example 5.2 We use our running example in Figure 2 to explain Definition 5.1 (the states are numbered according to this definition). For the abstract transition $t = (q_0, \mathsf{address}, q_1)$ we add the states $(t, 1)$ and $(t, 2)$ to Q_r ($(t, 0)$ and $(t, 3)$ correspond to states q_0 and q_1 respectively). T' consists of the transitions: $((t, 0), \mathsf{street}, (t, 1))$, $((t, 1), \mathsf{city}, (t, 2))$ and $((t, 2), \mathsf{postalcode}, (t, 3))$. In T_r we delete the address transition from the set of abstract transitions and we add T'. We add all labels from the refinement trace: $\{\mathsf{street}, \mathsf{city}, \mathsf{postalcode}\}$ to I_r and we delete the refinement label "address" (the output label set stays the same). □

Lemma 5.3 states that the prefix closure of the refined *Utraces* of the abstract specification equals the set of *Utraces* of the refined specification. This result holds because we defined trace refinement in such a way that the refinement of a trace results in a trace from the refined system. To include traces that end in the middle of the refinement, we apply the prefix closure.

Lemma 5.3 $\downarrow(Utraces(s)[r]) = Utraces(s[r])$

Lemma 5.4 states that for completely refined *Utraces* the set of outputs after the trace in the refined system equals the set of outputs in the abstract system after the contracted trace. This holds because r-complete traces end in states that come from the abstract system (old states). Because atomic linear input-inputs refinement does not add outputs to the refined system, the output behavior of the old states is not altered by the refinement.

Lemma 5.4 $\forall \sigma \in Utraces(s)[r] : out(s[r] \textbf{ after } \sigma) = out(s \textbf{ after } \sigma\langle r \rangle)$

For not completely refined *Utraces* (traces in $\downarrow(Utraces(s)[r]) \backslash Utraces(s)[r])$) Lemma 5.5 states that the only output of the refined specification after such a trace is quiescence. This holds because not r-complete utraces end inside the refinement (in new states). Because our refinement does not add outputs, the only allowed output inside the refinement is quiescence.

Lemma 5.5 $\forall \sigma \in \downarrow(Utraces(s)[r]) \backslash Utraces(s)[r] : out(s[r] \textbf{ after } \sigma) = \{\delta\}$

6 uioco$_r$ for testing refined systems

In this section we introduce the implementation relation **uioco**$_r$ that express correctness of the concrete implementation in terms of the abstract specification and the refinement pair. We show that **uioco**$_r$ is equivalent to the **uioco** relation over refined specifications.

Definition 6.1 [**uioco**$_r$] Let $s \in \mathcal{LTS}(I_1, U)$, $i \in \mathcal{IOTS}(I_2, U)$, $r = (a_r, \sigma_r)$, $I_2 = I_1 \backslash \{a_r\} \cup I(\sigma_r)$.

i **uioco**$_r$ $s =_{\text{def}}$ $\forall \sigma \in \downarrow(Utraces(s)[r])$:
if $\sigma \in Utraces(s)[r]$ then $out(i \textbf{ after } \sigma) \subseteq out(s \textbf{ after } \sigma\langle r \rangle)$
else $out(i \textbf{ after } \sigma) \subseteq \{\delta\}$

For completely refined *Utraces* the allowed output behavior of the implementation is restricted to the output behavior of the abstract specification after the contracted trace (see Lemma 5.4). For incompletely refined *Utraces* the allowed output behavior of the implementation is restricted to quiescence (see Lemma 5.5). Because of Lemma 5.3 we know that we have covered all possible traces of the refined specification.

The following theorem states the equality between **uioco**$_r$ and **uioco**. This equality follows directly from the lemma's discussed above.

Theorem 6.2 Let $s \in \mathcal{LTS}(I_1, U), i \in \mathcal{IOTS}(I_2, U)$, with $r = (a_r, \sigma_r)$, and $I_2 = I_1 \backslash \{a_r\} \cup I(\sigma_r)$

$$i \textbf{ uioco}_r \; s \Leftrightarrow i \textbf{ uioco } s[r]$$

Example 6.3 Let us look again at abstract and refined specification in Figure 2. To illustrate Definition 6.1 and Theorem 6.2 we use the following two traces: street·city·postalcode·store is a complete refinement of address·store and street·city an incomplete refinement. As we can see, both traces are in the set of *Utraces* of the refined specification, as stated in Lemma 5.3. The trace address·store leads us to state q_2 in the abstract specification and the trace

street·city·postalcode·store leads us to state q_2 in the refined specification. As we can see, the set of outputs is in both states the same, conform to Lemma 5.4. The r-incomplete trace street·city leads us to state $(t, 2)$ in the refined specification. This state is quiescent, as stated in Lemma 5.5. When we put these results together, we see that the $\mathbf{uioco}_r$ definition for the abstract specification is equal to the **uioco** definition for the refined specification. □

7 Test case refinement

In the previous sections we have shown how to obtain a refined test suite by refining the specification; from this refined specification we can generate a complete test suite. In this section we show how to refine existing abstract test cases, like the test cases shown in Figure 3. Furthermore, we show under what conditions the refinement of a complete abstract test suite results in a complete refined test suite with respect to $\mathbf{uioco}_r$.

To test inside the refinement we need several test cases (we can make several observations). Therefore we generate a set of mini test cases that test the entire behavior of the refined action. We replace transitions with the refinement label in the abstract test case with these mini test cases.

7.1 Generation of mini test cases

We present an algorithm to generate mini test cases that test the entire behavior inside the refinement. The algorithm is closely related to the test generation algorithm of Tretmans [5]. There are some minor differences:

1. The only pass state is at the end of a mini test case. A possible error can be anywhere within the refinement, so it is no use to stop testing before the end of the refinement.

2. There are no observations at the start and the end state of the mini test. Because atomic linear input-inputs refinement does not add or change output actions we use the observations of the abstract system in these states.

Definition 7.1 [Generation of mini tests] $MT \subseteq \mathcal{TEST}(L(\sigma_r), U_\delta)$, a set of mini tests, is obtained from σ_r (with respect to an input label set I and and output label set U) in the following way. The stimulus and response step are executed in a non-deterministic manner. Let $n = |\sigma_r|$ and $1 \leq i < n$.

Stimulus step t_i := $\sigma_r|_i; t_{i+1}$
Response step t_i := $\sigma_r|_i; (\Sigma\{x; \mathbf{fail} \mid x \in U\} \Box \delta; t_{i+1})$
Pass step t_n := $\sigma_r|_n; \mathbf{pass}$

MT is the set of mini tests that can be obtained from t_1: $MT = \{t_1\}$

The set of mini test is built with the process algebraic operators action prefix (;) and choice ($\Box$ and Σ) in the same style as Tretman's algorithm. For readers that are unfamiliar with this notation,formally we write this as follows:

Let t_i be test cases for $i = 1, 2$ and $\mu \in L_\delta$
; $(\mu; t_1) \xrightarrow{\mu} t_1$
$\Box$ if $t_1 \xrightarrow{\mu} t_1'$ then $t_1 \Box t_2 \xrightarrow{\mu} t_1'$ and $t_2 \Box t_1 \xrightarrow{\mu} t_1'$
Σ if $t_i \xrightarrow{\mu} t_i'$ for $i \in I$ then $\Sigma\{t_i \mid i \in I\} \xrightarrow{\mu} t_i'$

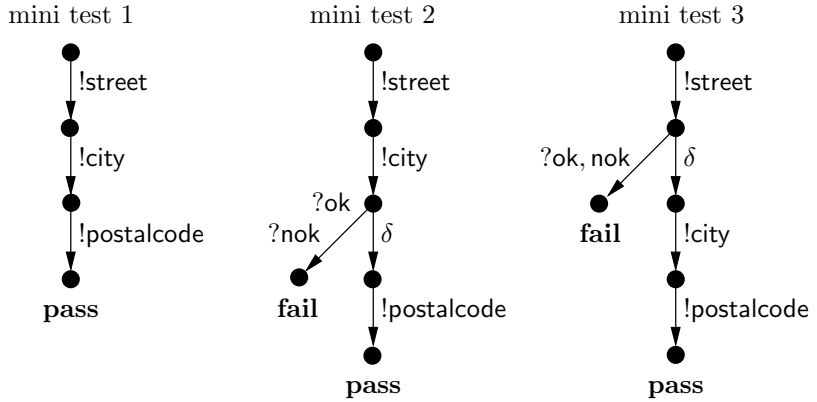

Figure 6: Generation of mini tests

Example 7.2 In Figure 6 we show three mini tests generated with the algorithm in Definition 7.1 for $\sigma_r = \mathsf{street}{\cdot}\mathsf{city}{\cdot}\mathsf{postalcode}$. Mini test 1 starts with a stimulus step: $t_1 := \mathsf{street}; t_2$, followed by again a stimulus step: $t_2 := \mathsf{city}; t_3$. After this only the pass step is possible: $t_3 := \mathsf{postalcode}; \mathbf{pass}$. This results in $t_1 := \mathsf{street}; \mathsf{city}; \mathsf{postalcode}; \mathbf{pass}$ which corresponds with the labeled transition system of mini test 1. Mini test 2 starts the same with the stimulus street: that is $t_1 := \mathsf{street}; t_2$. This step is followed by an observation step: $t_2 := \mathsf{city}; (\Sigma\{x; \mathbf{fail} \mid x \in U\} \Box \delta; t_3)$. This step leads to the stimulus city followed by the observations ok, nok both leading to a fail state. After the observation of quiescence the test continues with t_3. This is again the stimulus postalcode followed by pass. Mini test 3 is almost identical to mini test 2, except that it starts with an observation. □

7.2 Test case refinement

Test case refinement is similar to LTS refinement. The main difference is that test case refinement results in a *set* of refined test cases, where LTS refinement results in one transition system. The definition is explained in Example 7.4.

Definition 7.3 Given a test case $t = \langle Q_t, I_t, U_t, T_t, t_0, \mathbf{pass}_t, \mathbf{fail}_t \rangle$ and a refinement pair (a_r, σ_r) we define test case refinement as follows. Let MT be the set of mini tests generated with the algorithm from Definition 7.1. Let f be a function from Q_t to MT. For better readability we denote a mini test obtained from f for a state q as $f(q) = \langle Q_q, I_q, U_q, T_q, \mathrm{start}_q, \mathbf{pass}_q, \mathbf{fail}_q \rangle$. We assume all states in the images of f to be unique. In order to deal with mini tests of one transition (refinements of one transition) we use the following notational convention: $(q, q') = q$ if $q' \in \mathbf{pass}_{q'}$ and $(q, q') = q'$ if $q \in \mathrm{start}_q$
$t[r] = \{t[f] \mid f : Q_t \to MT\}$ where $t[f] = \langle Q_f, I_f, U_t, T_f, t_0, \mathbf{pass}_t, \mathbf{fail}_f \rangle$ is defined as follows.

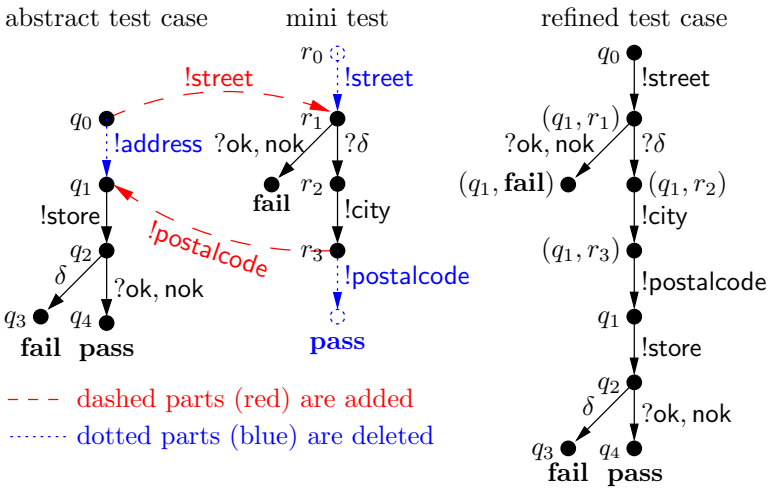

Figure 7: Example of test case refinement

$$
\begin{aligned}
&Q_f = Q_t \cup \{(q_2, q) \mid \exists q_1 \in Q_t : (q_1, a_r, q_2) \in T_t \wedge q \in Q_{q_2} \backslash (\mathbf{pass}_{q_2} \cup \{\mathrm{start}_{q_2}\})\} \\
&T_f = \{(q_1, \lambda, (q_2, q)) \mid (q_1, a_r, q_2) \in T_t \wedge (\mathrm{start}_{q_2}, \lambda, q) \in T_{q_2}\} \\
&\quad \cup \{((q_2, q), \lambda, q_2) \mid \exists q_1 \in Q_t : (q_1, a_r, q_2) \in T_t \wedge \exists q_3 \in \mathbf{pass}_{q_2} : (q, \lambda, q_3) \in T_{q_2}\} \\
&\quad \cup \{((q_2, q), \lambda, (q_2, q')) \mid \exists q_1 \in Q_t : (q_1, a_r, q_2) \in T_t \wedge (q, \lambda, q') \in T_{q_2} \wedge q \notin \mathrm{start}_{q_2} \\
&\qquad \wedge q' \notin \mathbf{pass}_{q_2}\} \\
&\quad \cup T_t \backslash \{(q_1, a_r, q_2) \in T_t \mid q_1, q_2 \in Q_t\} \\
&I_f = I_t \backslash \{a_r\} \cup I(\sigma_r) \\
&\mathbf{pass}_f = \mathbf{pass}_t \\
&\mathbf{fail}_f = \mathbf{fail}_t \cup \{(q_1, q_2) \in Q_f \mid q_1 \in Q_t \wedge q_2 \in \mathbf{fail}_{q_1}\}
\end{aligned}
$$

We apply a little mathematical trick with our function f. The function maps the states of the abstract test case to the set of mini tests. For every refinement label transition (q_1, a_r, q_2) we get a mini test $f(q_2)$. We replace the refinement label transition with this mini test. $t[f]$ results in one refined test case and when we combine all possible refinements with f we get a set of refined test cases in which a_r transitions are replaced with all possible mini tests. Our notational convention $(q, q') = q$ if $q' \in \mathbf{pass}_{q'}$ and $(q, q') = q'$ if $q \in \mathrm{start}_q$ enables us to deal with refinements of length one. We believe that this notation improves the readability of the definition as we do not have to introduce extra exceptions.

Example 7.4 [Test case refinement] In Figure 7 we show an abstract test case on the left, a mini test in the middle and the resulting refined test case on the right. We use different types of lines: dashed parts are added, dotted parts are deleted and solid parts remain unchanged.

We delete the refinement label transition, $(q_0, \mathsf{address}, q_1)$ from the abstract test case (dotted transition) and all other transitions are added to T_f. All states are copied to Q_f.

From the mini test we delete the start and pass states. All other states are added to Q_f as a pair with q_1. We delete the transitions from the start state and transitions leading to pass states and add all other transitions to T_f.

To finalize the test case refinement we let the first transition in the mini test start in q_0, the start state of the refinement transition: the dashed transition

labeled with street between q_0 and r_1. In a similar way we redirect the postalcode transition to the pass state to q_1. When we reorganize the dashed parts and the black solid parts we obtain the refined test case on the right. □

7.3 Completeness of test case refinement

When we generate a test suite from the refined specification with Tretmans test generation algorithm, we know that the test suite is complete with respect to **uioco** and $s[r]$ (result from Tretmans, see [4]). If we can show that the refinement of a complete test suite results in a complete refined test suite with respect to **uioco** and $s[r]$, we know that both test suites are equivalent with respect to completeness.

As usual we divide completeness in *soundness* and *exhaustiveness*. It turns out that to obtain soundness of a refined sound test suite we need an extra requirement. We call this requirement *"conformance trace safety"*. It expresses that a test trace that does not end in a fail state is a utrace of the specification.

Definition 7.5 Let $s \in \mathcal{LTS}(I,U), t \in \mathcal{TEST}(I,U)$. A test case t is conformance trace safe with respect to **uioco** and s when

$$t \xrightarrow{\sigma} q \notin \textbf{fail} \Rightarrow \sigma \in \mathit{Utraces}(s)$$

Test case refinement is defined in such a way that the refinement of a conformance trace safe and sound test case with respect to **uioco** and s leads to a sound refined test case with respect to **uioco** and $s[r]$.

Theorem 7.6 [Soundness of the refined test suite] Let $t \in \mathcal{TEST}(I,U), s \in \mathcal{LTS}(I,U), r = (a_r, \sigma_r)$ and let t be conformance trace safe w.r.t. **uioco** and s.

(t is **sound** w.r.t. **uioco** and s) $\Rightarrow$ ($t[r]$ is **sound** w.r.t. **uioco** and $s[r]$)

Intuitively this theorem can be explained as follows. Like with LTS refinement we have the property that completely refined *Utraces* of s end in states of the abstract test case, where the output behavior is completely determined by the abstract system (see Lemma 5.4). Soundness is guaranteed by the soundness of the abstract test case. Conformance trace safety ensures that a trace in the refined test case that does not lead to a fail state is indeed a utrace of $s[r]$. Not completely refined *Utraces* test the behavior of the refinement, where the output behavior is limited to quiescence (see Lemma 5.5). Not completely refined traces lead to states from the mini tests. It can be easily seen that mini tests generated with the algorithm in Definition 7.1 only lead to fail if the observed output is not quiescent.

It turns out that exhaustiveness of the refined test suite does not necessarily follow from exhaustiveness of the abstract test suite. When the abstract test suite fulfills the following property, exhaustiveness of the refined test suite holds.

Definition 7.7 Let $s \in \mathcal{LTS}(I,U)$ and $r = (a_r, \sigma_r)$. A test suite T r-covers a specification s (denoted $r\text{-cov}(T,s)$) if the following holds:

$$r\text{-cov}(T,s) =_{\text{def}} \forall(\sigma{\cdot}a_r) \in \mathit{Utraces}(s) : (\exists t \in T : t \xrightarrow{\sigma \cdot a_r})$$

The property states that a test suite T covers a specification s with respect to r if for every utrace of s ending in a_r, there is a test case in T that can perform this trace.

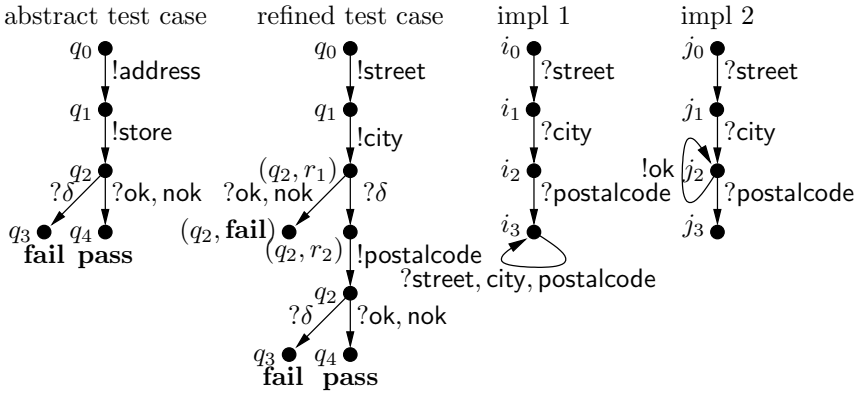

Figure 8: Figure to illustrate soundness and completeness properties

Theorem 7.8 [Exhaustiveness of the refined test suite] Let $s \in \mathcal{LTS}(I,U), T \subseteq \mathcal{TEST}(I,U), r = (a_r, \sigma_r)$ and r-cov(T,s) then
(T is **exhaustive** w.r.t. **uioco** and s) $\Rightarrow$ ($T[r]$ is **exhaustive** w.r.t. **uioco**$_r$ and s)

For exhaustiveness we follow the same line of thought as in the explanation of soundness. If the implementation is not **uioco**$_r$ correct there can be an error in the abstract behavior (from the abstract specification) or in the behavior of the refinement. In case of an error in the abstract behavior, we know that there is a test case that reveals the failure because the abstract test suite is exhaustive. In case of incorrectness in the refined part of the specification, we run into a problem. It may be that there is an error inside the refinement, but no abstract test case that leads to the refinement. The reason for this is that a complete test suite remains complete when deleting test cases that always lead to pass. The deleted test case may just be the test case that we need to obtain exhaustiveness. We can illustrate this as follows. Suppose that we have a specification that allows all behavior. A test suite with one test case that only consists of a **pass** state is complete. Refinement of this test suite results in the same test suite. Suppose that we have an implementation that can only perform the first refinement action and after that is not quiescent. This implementation is not **uioco**$_r$ correct, but the refined test suite does not have a test case to detect this.

For r-cov test suites exhaustiveness holds, because there always is an abstract test case that leads us to the refinement. Within the refinement only quiescence is allowed as output and because the implementation is not **uioco**$_r$ correct, we know that it is not quiescent. In the mini test generation algorithm we can easily see that such behavior leads to a fail verdict. We illustrate the soundness and exhaustiveness results with an example.

Example 7.9 Figure 8 shows an abstract test case (left), a refined test case and two implementations (right) for our data entry system. Both implementations have an error. Implementation 1 is quiescent in state i_3 and implementation 2 allows the output ok in state j_2.

For soundness we want to know if an error detected by a refined test case is indeed an error in the implementation. For implementation 1 we observe

quiescence after street, city and postalcode. Our test case leads to fail because it expects ok or nok as observation. Because the fail state is a state from the abstract test case and because we know that the abstract test case is sound, we also know that our refined test case is sound.

For implementation 2, the execution of the refined test case leads to a fail verdict after observing ok after street followed by city. This is a failure within the refinement ((q_2, **fail**) is a new state). Our observation within the refinement is ok and we know that the only allowed output within a refinement is δ. This means that the **fail** verdict is correct and that the test case is sound.

For exhaustiveness we can follow the same line of thought. Suppose the implementation is not **uioco** correct, like implementations 1 and 2, do we have a test case that detects the error? For implementation 1 this is clear: the error is in the abstract part of the system and because the abstract test suite is complete, there is a test case that tests the specific abstract state of the specification. Because this abstract test case is present, we know that the refined test case will detect the error. For an error inside a refinement, like in implementation 2 we have a problem, because it requires that there is an abstract test case that ends with address. As explained earlier, the existence of such a test case is guaranteed by completeness and r-completeness together, but not by completeness alone. □

At first sight it may be unclear if conformance trace safety can be met. The test case generation algorithm of Tretmans [5] fulfills this requirement (as it immediately gives the fail verdict when an observation is not allowed and it only tests with traces in $\mathcal{F}(s)$).

Corollary 7.10 A test suite generated with Tretmans algorithm for test case generation is conformance trace safe with respect to **uioco** and the abstract specification.

Likewise it may be unclear if the r-cov requirement for exhaustiveness can be met. The test case generation algorithm of Tretmans [5] fulfills this requirement (as it does not optimize test suites by deleting test cases); this is implied by Theorem 6.3 in [4].

Corollary 7.11 The refinement of a complete test suite generated with Tretmans algorithm for test case generation, is complete with respect to $\mathbf{uioco}_r$ and the abstract specification.

8 Conclusion

In this paper we have filled in the parts of our action refinement approach in Figure 1. We applied this approach to atomic linear input-inputs refinement. For this special case of action refinement we showed how to refine traces, transition systems and test cases. This enables us to obtain test cases with the required level of detail in an automated way. Furthermore we introduced the implementation relation $\mathbf{uioco}_r$ that relates the abstract specification to the concrete implementation by using the refinement information in the form of the refinement pair. We showed that a complete test suite can be derived from the

refined specification and under which conditions this test suite is equivalent to the refinement of a complete abstract test suite.

Related work In the light of conformance testing, the problem addressed by this paper is well known in practice and occurs often. However, no research has been carried out in the field of conformance testing nor in the field of action refinement.

In the context of action refinement, the results of Section 7 have an unexpected consequence. The vast majority of research in action refinement has concentrated on the so-called *coarsest congruence* question (given two equivalent specifications, are they still equivalent after refinement?). In this paper we are not primarily interested in equivalences at all: the core issue is conformance relation, embodied in **uioco**. Still, an obvious derived equivalence is that of *specification strength* — two specifications are equivalent if they are satisfied by the same set of systems. Surprisingly, this equivalence is *not* preserved even under atomic action refinement, as a side-effect of the fact that test case refinement does not always preserve completeness. This is in contrast to previously studied equivalences; see [2].

Future work This paper is only a first step; it treats a non-trivial though rather simple form of atomic action refinement. Future research focuses on arbitrary atomic refinement. This means that no actions are allowed to interfere with the refinement, but we drop the linearity and input-inputs constraints. As a result we allow branching (including looping) behavior with a mix of input and output actions. Arbitrary atomic refinement is the next research step. With arbitrary atomic refinement we will be able to refine the video game example from our introduction (Figure 4).

Some research has been done in comparing Finite State Machine (FSM) testing with LTS based testing [3]. With atomic action refinement we can refine the atomic input output pair from an FSM into two sequential actions. This might give an interesting basis for comparison.

A Proofs Section 7

To prevent confusion between the components of an abstract test case and a refined test case we use a subscript r to keep the two apart. For an abstract test case t we will use $t = \langle Q, I, U, T, \text{start}, \mathbf{pass}, \mathbf{fail}\rangle$ and for a refined test case $t_r \in t[r]$ we use $t_r = \langle Q_r, I_r, U_r, T_r, \text{start}_r, \mathbf{pass}_r, \mathbf{fail}_r\rangle$. Whenever necessary we will use the subscript r to prevent confusion.

We sometimes write $t \xrightarrow{\sigma} \mathbf{fail}$ to indicate that a test trace leads to an arbitrary fail state. We use the notation $\delta^?$ to denote zero or one times δ.

The following definition defines *delta desaturation*. This means that a series of consecutive delta's in a trace are replaced with one delta action.

Definition A.1 Delta desaturation replaces a consecutive sequence of δ's with one δ action. Let $\sigma \in L^*_\delta$.

$$\lfloor\sigma\rfloor = \begin{cases} 1)\ \epsilon & \text{if } \sigma = \epsilon \\ 2)\ \lfloor\sigma'\rfloor\cdot\mu & \text{if } \sigma = \sigma'\cdot\mu \wedge \mu \neq \delta \\ 3)\ \lfloor\sigma'\rfloor\cdot\delta & \text{if } \sigma \in \sigma'\cdot\delta^+ \wedge \nexists\sigma'' : \sigma' = \sigma''\cdot\delta \end{cases}$$

Lemma A.2 Let $t = \langle Q, I, U, T, q_0, \mathbf{pass}, \mathbf{fail}\rangle, q, q' \in Q$ and $\sigma \in L^*_\delta$.

$$q \xrightarrow{\sigma} q' \Leftrightarrow q \xrightarrow{\lfloor\sigma\rfloor} q'$$

Proof

Only if: Proof by induction on the length of σ

Basic step: $\sigma = \epsilon$. The lemma holds as $\lfloor\epsilon\rfloor = \epsilon$.

Induction step: Let $\sigma = \sigma'\cdot\lambda$ and assume that the lemma holds for σ'. We identify the following cases:

- $\lambda \in L$

  $q \xrightarrow{\sigma'\cdot\lambda} q'$
  $\Rightarrow$ ($*$ Definition $\longrightarrow$ $*$)
  $\exists q_1 \in Q : q \xrightarrow{\sigma'} q_1 \xrightarrow{\lambda} q'$
  $\Rightarrow$ ($*$ Induction $*$)
  $\exists q_1 \in Q : q \xrightarrow{\lfloor\sigma'\rfloor} q_1 \xrightarrow{\lambda} q'$
  $\Rightarrow$ ($*$ Definition $\longrightarrow$ $*$)
  $q \xrightarrow{\lfloor\sigma'\rfloor\cdot\lambda} q'$
  $\Rightarrow$ ($*$ Definition A.1 case 2 $*$)
  $q \xrightarrow{\lfloor\sigma'\cdot\lambda\rfloor} q'$

- $\lambda = \delta$. We identify two cases:

  1. σ ends on more than one consecutive δ actions. In this case $\lfloor\sigma'\cdot\lambda\rfloor = \lfloor\sigma'\rfloor$, because the sequence of δ actions is reduced to one δ action.

     $q \xrightarrow{\sigma'\cdot\lambda} q'$
     $\Rightarrow$ ($*$ Definition $\longrightarrow$ $*$)
     $\exists q_1 \in Q : q \xrightarrow{\sigma'} q_1 \xrightarrow{\lambda} q'$
     $\Rightarrow$ ($*$ Definition $\delta : q \xrightarrow{\delta} q$ $*$)
     $q \xrightarrow{\sigma'} q' \xrightarrow{\lambda} q'$
     $\Rightarrow$ ($*$ Induction $*$)
     $q \xrightarrow{\lfloor\sigma'\rfloor} q' \xrightarrow{\lambda} q'$
     $\Rightarrow$ ($*$ Premise: $\lfloor\sigma'\cdot\lambda\rfloor = \lfloor\sigma'\rfloor$ $*$)
     $q \xrightarrow{\lfloor\sigma'\cdot\lambda\rfloor} q'$

  2. σ ends on one delta action: λ. In this case $\lfloor\sigma'\rfloor\cdot\lambda = \lfloor\sigma'\cdot\lambda\rfloor$, because σ' does not end on a δ action. Therefore the final step changes to the following:

     $q \xrightarrow{\lfloor\sigma'\rfloor} q' \xrightarrow{\lambda} q'$
     $\Rightarrow$ ($*$ Definition $\longrightarrow$ $*$)
     $q \xrightarrow{\lfloor\sigma'\rfloor\cdot\lambda} q'$
     $\Rightarrow$ ($*$ Premise: $\lfloor\sigma'\cdot\lambda\rfloor = \lfloor\sigma'\rfloor\cdot\lambda$ $*$)
     $q \xrightarrow{\lfloor\sigma'\cdot\lambda\rfloor} q'$

If: Proof by induction on the length of σ

Basic step: $\sigma = \epsilon$. The lemma holds as $\lfloor\epsilon\rfloor = \epsilon$.

Induction step: Let $\sigma = \sigma'\cdot\lambda$ and assume that the lemma holds for σ'. We identify the following cases:

- $\lambda \in L$

  $q \xrightarrow{\lfloor \sigma' \cdot \lambda \rfloor} q'$
  $\Rightarrow$ ($*$ Definition A.1, $\lambda \neq \delta$ $*$)
  $q \xrightarrow{\lfloor \sigma' \rfloor \cdot \lambda} q'$
  $\Rightarrow$ ($*$ Definition $\longrightarrow$ $*$)
  $\exists q_1 \in Q : q \xrightarrow{\lfloor \sigma' \rfloor} q_1 \xrightarrow{\lambda} q'$
  $\Rightarrow$ ($*$ Induction $*$)
  $\exists q_1 \in Q : q \xrightarrow{\sigma'} q_1 \xrightarrow{\lambda} q'$
  $\Rightarrow$ ($*$ Definition $\longrightarrow$ $*$)
  $q \xrightarrow{\sigma' \cdot \lambda} q'$
- $\lambda = \delta$. We identify the following cases:
  1. σ ends on more than one δ action; so λ is part of a sequence of δ actions. In this case $\lfloor \sigma' \cdot \lambda \rfloor = \lfloor \sigma' \rfloor$.

     $q \xrightarrow{\lfloor \sigma' \cdot \lambda \rfloor} q'$
     $\Rightarrow$ ($*$ Premise: $\lfloor \sigma' \cdot \lambda \rfloor = \lfloor \sigma' \rfloor$ $*$)
     $q \xrightarrow{\lfloor \sigma' \rfloor} q'$
     $\Rightarrow$ ($*$ Induction $*$)
     $q \xrightarrow{\sigma'} q'$
  2. σ ends on one δ action, namely λ. In this case $\lfloor \sigma' \cdot \lambda \rfloor = \lfloor \sigma' \rfloor \cdot \lambda$.

     $q \xrightarrow{\lfloor \sigma' \cdot \lambda \rfloor} q'$
     $\Rightarrow$ ($*$ Premise: $\lfloor \sigma' \cdot \lambda \rfloor = \lfloor \sigma' \rfloor \cdot \lambda$ $*$)
     $q \xrightarrow{\lfloor \sigma' \rfloor \cdot \lambda} q'$
     $\Rightarrow$ ($*$ Definition $\longrightarrow$ $*$)
     $\exists q_1 \in Q : q \xrightarrow{\lfloor \sigma' \rfloor} q_1 \xrightarrow{\lambda} q'$
     $\Rightarrow$ ($*$ Induction $*$)
     $\exists q_1 \in Q : q \xrightarrow{\sigma'} q_1 \xrightarrow{\lambda} q'$
     $\Rightarrow$ ($*$ Definition $\longrightarrow$ $*$)
     $q \xrightarrow{\sigma' \cdot \lambda} q'$

□

The following lemma shows that the trace via which a sound and conformance trace safe test case leads to a fail state ends with an output action. Furthermore, except for the last output action, the trace is a utrace.

Lemma A.3 Let $t \in \mathcal{TEST}(I, U)$ be sound and conformance trace safe with respect to a specification $s \in \mathcal{LTS}(I, U)$ and **uioco**.

$$t \xrightarrow{\sigma} \textbf{fail} \Rightarrow \exists \sigma' \in \mathit{Utraces}(s), x \in U_\delta : \sigma' \cdot x = \sigma \wedge x \notin \mathit{out}(s \textbf{ after } \sigma)$$

Proof We first show that the trace σ ends with an output action. Next we proof the rest of the lemma. Suppose that σ does not end with an output action then it either

1. is the empty trace. This conflicts with the fact that $\epsilon \in \mathit{Utraces}(s)$.
2. ends with an input action. Suppose that $\sigma = \sigma' \cdot a$ with a an input action. Note that $t \xrightarrow{\sigma'} q \notin \textbf{fail}$ and $\sigma' \in \mathit{Utraces}(s)$ as t is conformance trace

safe. We now construct an implementation i such that $\forall \sigma \in Utraces(s) : out(i \textbf{ after } \sigma) \subseteq out(s \textbf{ after } \sigma)$. But we also implement the input action a after σ', so $\sigma' \cdot a \in Straces(i)$. According to **uioco** this is perfectly fine, as **uioco** allows arbitrary behavior for underspecified input actions. As a result we have created a **uioco** correct implementation. However we have a sound test case that gives a fail verdict. This conflicts with the fact that the test case is sound.

This means that the trace σ ends with an output action (including δ):

$\exists \sigma' \in L^*_\delta, x \in U_\delta : t \xrightarrow{\sigma' \cdot x} \textbf{fail}$
$\Rightarrow$ $(*$ Definition $\longrightarrow$ $*)$
$\exists \sigma' \in L^*_\delta, x \in U_\delta, q_1 \in Q : t \xrightarrow{\sigma'} q_1 \xrightarrow{x} \textbf{fail}$
$\Rightarrow$ $(*$ t is conformance trace safe. Fail states are final $*)$
$\exists \sigma' \in Utraces(s), x \in U_\delta, q_1 \in Q : t \xrightarrow{\sigma'} q_1 \xrightarrow{x} \textbf{fail}$
$\Rightarrow$ $(*$ t is sound $*)$
$\exists \sigma' \in Utraces(s), x \in U_\delta, q_1 \in Q : t \xrightarrow{\sigma'} q_1 \xrightarrow{x} \textbf{fail} \wedge \sigma' \cdot x \notin Utraces(s)$
$\Rightarrow$ $(*$ Definition $out()$, **after** $*)$
$\exists \sigma' \in Utraces(s), x \in U_\delta : x \notin out(s \textbf{ after } \sigma')$
$\Rightarrow$ $(*$ Premise: $\sigma = \sigma' \cdot x$ $*)$
$\exists \sigma' \in Utraces(s), x \in U_\delta : \sigma = \sigma' \cdot x \wedge x \notin out(s \textbf{ after } \sigma')$

□

We repeat the following lemmas that we reuse from other papers.

Lemma 5.3 Let $s \in \mathcal{LTS}(I,U), r = (a_r, \sigma_r)$.

$$\downarrow(Utraces(s)[r]) = Utraces(s[r])$$

Proof For the proof we refer to [6] (Proposition C.7). □

Lemma 5.4 Let $s \in \mathcal{LTS}(I,U), r = (a_r, \sigma_r)$.

$$\forall \sigma \in Utraces(s)[r] : out(s[r] \textbf{ after } \sigma) = out(s \textbf{ after } \sigma\langle r \rangle)$$

Proof For the proof we refer to [6] (Proposition C.8). □

Lemma 5.5 $s \in \mathcal{LTS}(I,U), \sigma \in \downarrow(Utraces(s)[r]) \setminus Utraces(s)[r], r = (a_r, \sigma_r)$.

$$out(s[r] \textbf{ after } \sigma) \subseteq \{\delta\}$$

Proof For the proof we refer to [6] (Proposition C.9). □

Proposition A.4 Let $\sigma \in L^*_\delta[r], r = (a_r, \sigma_r)$

$$\sigma \in \sigma\langle r \rangle[r]$$

Proof For the proof we refer to [6] (Proposition 4.9). □

Lemma A.5 $s \in \mathcal{LTS}(I,U), \sigma \in \downarrow(Utraces(s)[r]) \setminus Utraces(s)[r], r = (a_r, \sigma_r)$

$\exists \sigma_1, \sigma_2, \sigma_3 \in L^*_{r\delta} : \sigma = \sigma_1 \cdot \sigma_2 \wedge \sigma_2 \cdot \sigma_3 \in \lceil \sigma_r \rceil \wedge \mathbf{rc}_r(\sigma_1) \wedge \sigma_1 \cdot \sigma_2 \cdot \sigma_3 \in Utraces(s)[r]$

Proof For the proof we refer to [6] (follows from the proof of Lemma C.6). □

Lemma A.6 Let $\sigma \in L^*_{r\delta}, \lambda \in L_{r\delta}, r = (a_r, \sigma_r)$ and $\mathbf{rc}_r(\sigma{\cdot}\lambda)$. There are two possibilities for the form of $\sigma{\cdot}\lambda$

1. $\lambda \in L_{r\delta} \backslash L(\sigma_r) \wedge \nexists \sigma_1, \sigma_2 \in L^*_{r\delta} : \sigma = \sigma_1{\cdot}\sigma_2 \wedge \sigma_2{\cdot}\lambda \in \downarrow\lceil\sigma_r\rceil \wedge \mathbf{rc}_r(\sigma)$
2. $\lambda = \sigma_r|_n \wedge \exists \sigma_1, \sigma_2 \in L_{r\delta} : \sigma = \sigma_1{\cdot}\sigma_2 \wedge \sigma_2{\cdot}\lambda \in \lceil\sigma_r\rceil \wedge \mathbf{rc}_r(\sigma_1)$

Proof For the proof we refer to [6] (Lemma A.1). □

Lemma A.7 Let $s \in \mathcal{LTS}(I, U), L = I \cup U, \sigma \in L^*_\delta$

$$out(s \textbf{ after } \sigma) = out(s \textbf{ after } \lfloor\sigma\rfloor)$$

Proof This proof follows straightforward from the definition of δ. $q \xrightarrow{\delta} q$ stands for the absence of any transition $q \xrightarrow{\mu} q'$ with $\mu \in U_\tau$. As a result a sequence of delta actions in a trace stay in the same state without enabling any new transitions. □

The following three lemmas clarify the form of traces that a mini-test can perform.

Lemma A.8 Let $r = (a_r, \sigma_r), mt = \langle Q, L(\sigma_r), U, T, \mathbf{pass}, \mathbf{fail}\rangle \in MT, n = |\sigma_r|, 1 \leq i < n, q \in Q\backslash(\mathbf{pass} \cup \mathbf{fail})$

$$mt \xrightarrow{\sigma} q \quad \Leftrightarrow \quad \sigma \in \downarrow\sigma_r|_1{\cdot}\delta^? \cdots \sigma_r|_{n-1}{\cdot}\delta^? \tag{7}$$

$$mt \xrightarrow{\sigma} \mathbf{fail} \quad \Leftrightarrow \quad \sigma \in \sigma_r|_1{\cdot}\delta^? \cdots \delta^?{\cdot}\sigma_r|_i{\cdot}U \tag{8}$$

$$mt \xrightarrow{\sigma} \mathbf{pass} \quad \Leftrightarrow \quad \sigma \in \sigma_r|_1{\cdot}\delta^? \cdots \delta^?{\cdot}\sigma_r|_n \tag{9}$$

Proof

Only if: We start with the proof of Equation (7) and Equation (8). We use the following equation in our proof. Let $1 \leq i < n$ and let t_i refer to the set of mini-tests generated in step i in the mini test case generation algorithm (Definition 7.1).

$$\begin{aligned} &\forall t \in t_1, \exists t' \in t_{i+1}, \sigma \in \sigma_r|_1{\cdot}\delta^? \cdots \delta^?{\cdot}\sigma_r|_i : \\ &\quad (\exists \sigma' \in \delta^? : t \xrightarrow{\sigma{\cdot}\sigma'} t' \vee \forall y \in U : t \xrightarrow{\sigma{\cdot}y} \mathbf{fail}) \end{aligned} \tag{10}$$

Basic step: $i = 1$. From Definition 7.1 (mini test generation) two rules apply:

1. Stimulus step: $t_1 = \sigma_r|_1; t_2$.
2. Response step: $t_1 = \sigma_r|_1; (\Sigma\{x; \mathbf{fail} \mid x \neq \delta\}\Box\delta; t_2)$.

Taking step 1 and 2 together we see that for $\forall t \in t_1, \exists \sigma' \in \delta^? : t \xrightarrow{\sigma_r|_1{\cdot}\sigma'} t_2 \vee \forall y \in U : t \xrightarrow{\sigma_r|_1{\cdot}y} \mathbf{fail}$. Note that the fail state is a final state; there are no transitions that leave this state.

Induction step: Assume that the lemma holds for $1 \leq j < i$. Let $1 \leq i < n$. From the definition of a mini test, we see that two rules may apply for test step i:

1. Stimulus step $(1 \leq i < n)$: $t_i = \sigma_r|_i; t_{i+1}$.

2. Response step ($1 \leq i < n$): $t_i = \sigma_r|_i; (\Sigma\{x; \mathbf{fail} \mid x \neq \delta\}\Box\delta; t_{i+1})$.

For step $j+1$ we get the following result (note that $1 < j+1 < n$): $\exists \sigma' \in \delta^? : t_{j+1} \xrightarrow{\sigma_r|_{j+1} \cdot \sigma'} t_{j+2}$ or $\forall y \in U : t_{j+1} \xrightarrow{y} \mathbf{fail}$. When we combine this with the induction hypothesis we get: $\forall t \in t_1, \exists t' \in t_{j+2}, \sigma \in \sigma_r|_1 \cdot \delta^? \cdots \delta^? \cdot \sigma_r|_{j+1} : (\exists \sigma' \in \delta^? : t \xrightarrow{\sigma \cdot \sigma'} t' \vee \forall y \in U : t \xrightarrow{\sigma \cdot y} \mathbf{fail})$. The first part of the disjunction proves Equation (7) and the second part proves Equation (8).

When we add the last step of the mini test generation algorithm we see:

1. Concluding step ($i = n$). $t_n = \sigma_r|_n \cdot \mathbf{pass}$.

This means that $\forall t \in t_1, \exists \sigma \in \sigma_r|_1 \cdot \delta^? \cdots \delta^? \cdot \sigma_r|_n : t \xrightarrow{\sigma} \mathbf{pass}$ and this proves Equation (9).

If: The other way around we need to universally quantify over the possible traces instead of over the mini tests. Therefore we use the following equations. Let $1 \leq i < n$:

$$\forall \sigma \in \sigma_r|_1 \cdot \delta^? \cdots \sigma_r|_i \cdot \delta^?, \exists t \in t_1, t' \in t_{i+1} \notin \mathbf{pass} \cup \mathbf{fail} : \quad t \xrightarrow{\sigma} t' \quad (11)$$

$$\forall \sigma \in \sigma_r|_1 \cdot \delta^? \cdots \sigma_r|_i \cdot U, \exists t \in t_1 : \quad t \xrightarrow{\sigma} \mathbf{fail} \quad (12)$$

$$\forall \sigma \in \sigma_r|_1 \cdot \delta^? \cdots \delta^? \cdot \sigma_r|_n, \exists t \in t_1 : \quad t \xrightarrow{\sigma} \mathbf{pass} \quad (13)$$

The proof of these equations is similar to the proofs in the only if case.

□

You may wonder whether it is enough to generate only one δ in the mini-test generation algorithm. Because of the definition of quiescence it does not matter if we have one or several observations of quiescence (if you observe quiescence once, you can observe it till infinity; $q \xrightarrow{\delta} q$ means $\forall x \in U_\tau : q \not\xrightarrow{x}$). Furthermore, Lemma A.7 shows that the output behavior of states is not changed.

The following two lemmas relate the abstract test case and the refined test case for single transitions (in the abstract test case).

Lemma A.9 Let $t = \langle Q, I, U, T, q_0, \mathbf{pass}, \mathbf{fail} \rangle \in \mathcal{TEST}(I, U), q, q' \in Q, \lambda \in L_\delta \backslash \{a_r\}, t_r \in t[r], r = (a_r, \sigma_r)$

$$q \xrightarrow{\lambda} q' \Leftrightarrow q \xrightarrow{\lambda}_r q'$$

Proof

Only if:

$$\begin{array}{ll} & q \xrightarrow{\lambda} q' \\ \Rightarrow & (* \text{ Definition test case refinement: } \lambda \neq a_r \ *) \\ & \forall t_r \in t[r] : q \xrightarrow{\lambda}_r q' \end{array}$$

If:

$$\begin{array}{ll} & q \xrightarrow{\lambda}_r q' \\ \Rightarrow & (* \text{ Definition test case refinement } (\lambda \notin L(\sigma_r), q, q' \in Q) \ *) \\ & q \xrightarrow{\lambda} q \end{array}$$

Note that it is by the definition of test case refinement impossible to have a transition originating from a mini-test with the starting and ending state an abstract state (in Q). That is except for refinements consisting of a single action, but these are ruled out by $\lambda \in L_\delta \backslash \{a_r\}$. This also rules out δ transitions in the mini test.

□

Lemma A.10 Let $r = (a_r, r), t = \langle Q, I, U, T, \text{start}, \textbf{pass}, \textbf{fail}\rangle, q, q' \in Q, t_r \in t[r], (q, a_r, q') \in T$.

$$q \xrightarrow{a_r} q' \Leftrightarrow \exists \sigma \in \sigma_r|_1 \cdot \delta^? \cdots \delta^? \cdot \sigma_r|_n : q \xrightarrow{\sigma}_r q'$$

Proof

Only if: From Definition 7.3 it is clear that the transition (q, a_r, q') is replaced with a mini-test case of which the transition from the start state is connected to q and the transition that leads to the pass state is connected to q'. This means that in the refined test case the traces between q and q' are restricted by the set of traces that a mini-test can do between its start and pass state. Equation (9) in Lemma A.8 shows that this set of traces is $\sigma_r|_1 \cdot \delta^? \cdots \delta^? \cdot \sigma_r|_n$.

If: This follows immediately from equation Equation (9) in Lemma A.8 and Definition 7.3.

□

Lemma A.11 Let $t = \langle Q, I, U, T, \text{start}, \textbf{pass}, \textbf{fail}\rangle \in \mathcal{TEST}(I, U), t_r \in t[r], r = (a_r, r), \lambda \in L \backslash \{a_r\}$

$$q \xrightarrow{\lambda}_r q' \Rightarrow q, q' \in Q$$

Proof This follows immediately from the Definition 7.3; only transitions with the a_r label are altered.

□

Lemma A.12 Let $t = \langle Q, I, U, T, \text{start}, \textbf{pass}, \textbf{fail}\rangle \in \mathcal{TEST}(I, U), t_r \in t[r], q \in Q_r, r = (a_r, \sigma_r)$

$$q \xrightarrow{\sigma_r|_n}_r q' \Rightarrow q' \in Q$$

Proof This follows immediately from the Definition 7.3 and Equation (9) in Lemma A.8. The transition with $q \xrightarrow{a_r} q'$ is replaced with a mini test, where the pass state is replaced with q'. □

Lemma A.13 Let $r = (a_r, \sigma_r), t = \langle Q, I, U, T, \text{start}, \textbf{pass}, \textbf{fail}\rangle, q \in Q, n = |\sigma_r|, 1 \leq i < n, \sigma \in \sigma_r|_1 \cdot \delta^? \cdots \delta^? \cdot \sigma_r|_i, x \in U$.

$$q \xrightarrow{a_r} \Leftrightarrow \exists t_r \in t[r] : q \xrightarrow{\sigma \cdot x}_r \textbf{fail}$$

Proof

Only if: From Definition 7.3 (test case refinement) we know that an a_r transition is replaced with a mini test. From Equation (8) in Lemma A.8 we know that for traces in $\sigma_r|_1 \cdot \delta^? \cdots \delta^? \cdot \sigma_r|_i \cdot U$ with $1 \leq i < n = |\sigma_r|$ there is a mini test that will lead to a fail state.

If: Because of Definition 7.3 and Definition 7.1 we know that only a refinement, or more precisely, a mini test starts with $\sigma_r|_1$. From Equation (8) in Lemma A.8 we know that all mini tests lead that can perform the trace $\sigma{\cdot}x$ lead to fail. Combining these we know that $q \xrightarrow{a_r}$

□

The following is a technical lemma that is used in Lemma A.15. It specifies the form of a trace (from a refined test case) between two 'old' states (from the set of states of the abstract test case) where the trace does not encounter any other 'old' states.

Lemma A.14 Let $t = \langle Q, I, U, T, q_0, \mathbf{pass}, \mathbf{fail}\rangle \in \mathcal{TEST}(I,U), t_r \in t[r]$ with $q, q' \in Q, r = (a_r, \sigma_r)$
$q \xrightarrow{\sigma}_r q' \wedge (\nexists q_1 \in Q, \sigma_1, \sigma_2 \in L^+_{r\delta} : \sigma = \sigma_1{\cdot}\sigma_2 \wedge q \xrightarrow{\sigma_1}_r q_1 \xrightarrow{\sigma_2}_r q')$
$\Rightarrow (\sigma \in L_{r\delta}\backslash L(\sigma_r) \vee \sigma \in \sigma_r|_1{\cdot}\delta^?\cdots\delta^?{\cdot}\sigma_r|_n)$

Proof Let MT denote the set of mini-tests generated with the algorithm in Definition 7.1.

$q \xrightarrow{\sigma}_r q' \wedge (\nexists q_1 \in Q, \sigma_1, \sigma_2 \in L^+_{r\delta} : \sigma = \sigma_1{\cdot}\sigma_2 \wedge q \xrightarrow{\sigma_1}_r q_1 \xrightarrow{\sigma_2}_r q')$
$\Rightarrow$ ($*$ Definition 7.3, note that $L_\delta\backslash\{a_r\} = L_{r\delta}\backslash L(\sigma_r)$ $*$)
$\sigma \in L_{r\delta}\backslash L(\sigma_r) \vee \exists mt \in MT : mt \xrightarrow{\sigma} \mathbf{pass}$
$\Rightarrow$ ($*$ Lemma A.8 Equation (9) $*$)
$\sigma \in L_{r\delta}\backslash L(\sigma_r) \vee \sigma \in \sigma_r|_1{\cdot}\delta^?\cdots\delta^?{\cdot}\sigma_r|_n$

□

Lemma A.15 Let $r = (a_r, \sigma_r), t_r \in t[r], q \in Q$

$$q \xrightarrow{\sigma}_r q' \Rightarrow (\mathbf{rc}_r(\sigma) \Leftrightarrow q' \in Q)$$

Proof

Only if: To be proven: $q \xrightarrow{\sigma}_r q' \wedge \mathbf{rc}_r(\sigma) \Rightarrow q' \in Q$. Proof by induction on the structure of σ.

Because of Lemma A.6 and the definition of r-completeness, an r-complete trace σ is either the empty trace, or it exists of at least one label with the following form. Let $\sigma = \sigma'{\cdot}\lambda$ with $\sigma \in L^*_{r\delta}, \lambda \in L_{r\delta}$.

1. $\lambda \in L_{r\delta}\backslash L(\sigma_r) \wedge \mathbf{rc}_r(\sigma') \wedge \nexists \sigma_1, \sigma_2 \in L^*_{\sigma_r\delta} : \sigma = \sigma_1{\cdot}\sigma_2 \wedge \sigma_2{\cdot}\lambda \in \downarrow\lceil\sigma_r\rceil$
2. $\lambda = \sigma_r|_n \wedge \exists \sigma_1, \sigma_2 \in L^*_{r\delta} : \sigma = \sigma_1{\cdot}\sigma_2 \wedge \sigma_2 \in \lceil\sigma_r\rceil$

Basic Step: $\sigma = \epsilon$. There are no τ steps in a test case. Therefore $q \xrightarrow{\epsilon}_r q'$ implies $q = q'$ and therefore $q' \in Q$.

Induction Step: Assume that $\sigma = \sigma_1{\cdot}\sigma_2$ and that the lemma holds for σ_1 (note that $\mathbf{rc}_r(\sigma_1)$). We identify the following cases for σ_2:

1. $\sigma_2 = \lambda \in L_r\backslash L(\sigma_r)$
   $q \xrightarrow{\sigma_1{\cdot}\sigma_2}_r q'$
   $\Rightarrow$ ($*$ Definition $\longrightarrow$ $*$)
   $\exists q_1 \in Q_{t_r} : q \xrightarrow{\sigma_1}_r q_1 \xrightarrow{\sigma_2}_r q'$
   $\Rightarrow$ ($*$ Induction hypothesis $*$)
   $\exists q_1 \in Q : q \xrightarrow{\sigma_1}_r q_1 \xrightarrow{\sigma_2}_r q'$
   $\Rightarrow$ ($*$ Lemma A.11 $*$)
   $q' \in Q$

2. $\sigma_2 = \delta$

$q \xrightarrow{\sigma_1 \cdot \sigma_2}_r q'$

$\Rightarrow$ $(*$ Definition $\longrightarrow$ $*)$

$\exists q_1 \in Q_{t_r} : q \xrightarrow{\sigma_1}_r q_1 \xrightarrow{\sigma_2}_r q'$

$\Rightarrow$ $(*$ Induction hypothesis $*)$

$\exists q_1 \in Q_t : q \xrightarrow{\sigma_1}_r q_1 \xrightarrow{\sigma_2}_r q'$

$\Rightarrow$ $(*$ Definition δ $*)$

$q' \in Q$

3. $\sigma_2 \in \lceil \sigma_r \rceil$

$q \xrightarrow{\sigma_1 \cdot \sigma_2}_r q'$

$\Rightarrow$ $(*$ Definition $\lceil \sigma_r \rceil$ $*)$

$q \xrightarrow{\sigma_1 \cdot \sigma_r|_1 \cdot \delta^* \cdots \delta^* \cdot \sigma_r|_n}_r q'$

$\Rightarrow$ $(*$ Lemma A.12 $*)$

$q' \in Q$

If: $q \xrightarrow{\sigma}_r q' \wedge q' \in Q_t \Rightarrow \mathbf{rc}_r(\sigma)$

Proof by induction on the number of abstract states that σ encounters between q and q'.

Basic step: There are no intermediate abstract states between q and q'.

$q \xrightarrow{\sigma}_r q' \wedge (\nexists q_1 \in Q, \sigma_1, \sigma_2 \in L^+_{r\delta} : \sigma = \sigma_1 \cdot \sigma_2 \wedge q \xrightarrow{\sigma_1}_r q_1 \xrightarrow{\sigma_2}_r q')$

$\Rightarrow$ $(*$ Lemma A.14 $*)$

$\sigma \in L_{r\delta} \backslash L(\sigma_r) \vee \sigma \in \lceil \sigma_r \rceil$

$\Rightarrow$ $(*$ Definition r-complete $*)$

$\mathbf{rc}_r(\sigma)$

The case where $\sigma = \delta$ might not immediately clear, as δ might be in $\downarrow\lceil \sigma_r \rceil$. However because of the construction of a refined test case, this is not possible as $q, q' \in Q$.

Induction step: Suppose that the lemma holds for n intermediate abstract states. Let $q_1 \in Q, \sigma = \sigma_1 \cdot \sigma_2$ such that $q \xrightarrow{\sigma_1}_r q_1$ encounters n abstract states and there are no intermediate abstract states in $q_1 \xrightarrow{\sigma_2}_r q'$.

$q \xrightarrow{\sigma_1}_r q_1 \xrightarrow{\sigma_2}_r q'$

$\Rightarrow$ $(*$ Induction hypothesis $*)$

$\mathbf{rc}_r(\sigma_1) \wedge q_1 \xrightarrow{\sigma_2}_r q'$

$\Rightarrow$ $(*$ Basic step $*)$

$\mathbf{rc}_r(\sigma_1) \wedge (\sigma_2 \in L_{r\delta} \backslash L(\sigma_r) \vee \sigma_2 \in \lceil \sigma_r \rceil$

$\Rightarrow$ $(*$ Definition r-completeness $*)$

$\mathbf{rc}_r(\sigma_1 \cdot \sigma_2)$

$\Rightarrow$ $(*$ $\sigma = \sigma_1 \cdot \sigma_2$ $*)$

$\mathbf{rc}_r(\sigma)$

□

Lemma A.16 Let $r = (a_r, \sigma_r), t \in \mathcal{TEST}(I, U), q, q' \in Q, \sigma \in L^*_\delta, \sigma' \in \sigma[r]$.

$$q \xrightarrow{\sigma} q' \Leftrightarrow \exists t_r \in t[r] : q \xrightarrow{\lfloor \sigma' \rfloor}_r q'$$

Proof

Only if: Proof by induction on the length of σ

Basic step: $\sigma = \epsilon$. There are no τ-steps in test cases. Therefore $q = q'$ and the lemma trivially holds.

Induction step: Let $\sigma = \sigma_1 \cdot \lambda$ and assume that the lemma holds for σ_1. Following the definition of trace refinement we identify three cases:

1. $\lambda \in L \backslash \{a_r\}$

$$
\begin{array}{ll}
 & q \xrightarrow{\sigma_1 \cdot \lambda} q' \\
\Rightarrow & (* \text{ Definition } \longrightarrow \ *) \\
 & \exists q_1 \in Q : q \xrightarrow{\sigma_1} q_1 \xrightarrow{\lambda} q' \\
\Rightarrow & (* \text{ Induction } *) \\
 & \forall \sigma_1' \in \sigma_1[r], \exists t_r \in t[r], q_1 \in Q : q \xrightarrow{\lfloor \sigma_1' \rfloor}_r q_1 \wedge q_1 \xrightarrow{\lambda} q' \\
\Rightarrow & (* \text{ Lemma A.9 } *) \\
 & \forall \sigma_1' \in \sigma_1[r], \exists t_r \in t[r], q_1 \in Q : q \xrightarrow{\lfloor \sigma_1' \rfloor}_r q_1 \wedge q_1 \xrightarrow{\lambda}_r q' \\
\Rightarrow & (* \text{ Definition } \longrightarrow, \lambda \neq \delta \ *) \\
 & \forall \sigma_1' \in \sigma_1[r], \exists t_r \in t[r] : q \xrightarrow{\lfloor \sigma_1' \cdot \lambda \rfloor}_r q' \\
\Rightarrow & (* \text{ Definition trace refinement } *) \\
 & \forall \sigma' \in (\sigma_1 \cdot \lambda)[r], \exists t_r \in t[r] : q \xrightarrow{\lfloor \sigma' \rfloor}_r q' \\
\Rightarrow & (* \ \sigma = \sigma_1 \cdot \lambda \ *) \\
 & \forall \sigma' \in \sigma[r], \exists t_r \in t[r] : q \xrightarrow{\lfloor \sigma' \rfloor}_r q'
\end{array}
$$

2. $\lambda = \delta$.

$$
\begin{array}{ll}
 & q \xrightarrow{\sigma_1 \cdot \lambda} q' \\
\Rightarrow & (* \text{ Definition } \longrightarrow \ *) \\
 & q \xrightarrow{\sigma_1} q' \xrightarrow{\lambda} q' \\
\Rightarrow & (* \text{ Induction } *) \\
 & \forall \sigma_1' \in \sigma_1[r], \exists t_r \in t[r] : q \xrightarrow{\lfloor \sigma_1' \rfloor}_r q' \wedge q' \xrightarrow{\lambda} q' \\
\Rightarrow & (* \text{ Lemma A.9 } *) \\
 & \forall \sigma_1' \in \sigma_1[r], \exists t_r \in t[r] : q \xrightarrow{\lfloor \sigma_1' \rfloor}_r q' \wedge q' \xrightarrow{\lambda}_r q'
\end{array}
$$

We identify the following cases.

- σ_1' ends with one or more δ actions. In this case $\lfloor \sigma_1' \cdot \lambda \rfloor = \lfloor \sigma_1 \rfloor$.

$$
\begin{array}{ll}
\Rightarrow & (* \text{ Premise: } \lfloor \sigma_1' \cdot \lambda \rfloor = \lfloor \sigma_1' \rfloor \ *) \\
 & \forall \sigma_1' \in \sigma_1[r], \exists t_r \in t[r] : q \xrightarrow{\lfloor \sigma_1' \cdot \lambda \rfloor}_r q' \\
\Rightarrow & (* \text{ Definition trace refinement } *) \\
 & \forall \sigma' \in (\sigma_1 \cdot \lambda)[r], \exists t_r \in t[r] : q \xrightarrow{\lfloor \sigma' \rfloor}_r q' \\
\Rightarrow & (* \ \sigma = \sigma_1 \cdot \lambda \ *) \\
 & \forall \sigma' \in \sigma[r], \exists t_r \in t[r] : q \xrightarrow{\lfloor \sigma' \rfloor}_r q'
\end{array}
$$

- σ_1' does not end with a δ action. In this case $\lfloor \sigma_1' \rfloor \cdot \lambda = \lfloor \sigma_1' \cdot \lambda \rfloor$

$\Rightarrow$ ($*$ Definition $\longrightarrow$ $*$)
$\forall \sigma_1' \in \sigma_1[r], \exists t_r \in t[r] : q \xrightarrow{\lfloor \sigma_1' \rfloor \cdot \lambda}_r q'$
$\Rightarrow$ ($*$ Premise: $\lfloor \sigma_1' \rfloor \cdot \lambda = \lfloor \sigma_1' \cdot \lambda \rfloor$ $*$)
$\forall \sigma_1' \in \sigma_1[r], \exists t_r \in t[r] : q \xrightarrow{\lfloor \sigma_1' \cdot \lambda \rfloor}_r q'$
$\Rightarrow$ ($*$ Definition trace refinement $*$)
$\forall \sigma' \in (\sigma_1 \cdot \lambda)[r], \exists t_r \in t[r] : q \xrightarrow{\lfloor \sigma' \rfloor}_r q'$
$\Rightarrow$ ($*$ $\sigma = \sigma_1 \cdot \lambda$ $*$)
$\forall \sigma' \in \sigma[r], \exists t_r \in t[r] : q \xrightarrow{\lfloor \sigma' \rfloor}_r q'$

3. $\lambda = a_r$
$q \xrightarrow{\sigma_1 \cdot \lambda} q'$
$\Rightarrow$ ($*$ Definition $\longrightarrow$ $*$)
$\exists q_1 \in Q_t : q \xrightarrow{\sigma_1} q_1 \xrightarrow{\lambda} q'$
$\Rightarrow$ ($*$ Induction $*$)
$\forall \sigma_1' \in \sigma_1[r], \exists t_r \in t[r], q_1 \in Q_t : q \xrightarrow{\lfloor \sigma_1' \rfloor}_r q_1 \wedge q_1 \xrightarrow{\lambda} q'$
$\Rightarrow$ ($*$ Lemma A.10 $*$)
$\forall \sigma_1' \in \sigma_1[r], \exists t_r \in t[r], q_1 \in Q_t : q \xrightarrow{\lfloor \sigma_1' \rfloor}_r q_1$
$\wedge \forall \sigma_2 \in \lambda[r] : q_1 \xrightarrow{\lfloor \sigma_2 \rfloor}_r q'$
$\Rightarrow$ ($*$ Definition $\longrightarrow$, note that σ_2 does not start with δ $*$)
$\forall \sigma_1' \in \sigma_1[r], \forall \sigma_2 \in \lambda[r], \exists t_r \in t[r] : q \xrightarrow{\lfloor \sigma_1' \cdot \sigma_2 \rfloor}_r q'$
$\Rightarrow$ ($*$ Definition trace refinement $*$)
$\forall \sigma_1'' \in (\sigma_1 \cdot \lambda)[r], \exists t_r \in t[r] : q \xrightarrow{\lfloor \sigma_1'' \rfloor}_r q'$
$\Rightarrow$ ($*$ $\sigma = \sigma_1 \cdot \lambda$ $*$)
$\forall \sigma_1'' \in \sigma[r], \exists t_r \in t[r] : q \xrightarrow{\lfloor \sigma_1'' \rfloor}_r q'$

If: Proof by induction on the structure of σ'. From Lemma A.6 we know that there are two possibilities for the structure of non-empty rcomplete traces. From the definition of trace refinement we know that an rcomplete trace can also be empty. Therefore we distinguish the following cases.

1. $\sigma' = \epsilon$. There are no τ-steps in test cases, therefore $q = q'$ which trivially holds.

2. $\sigma' = \sigma_1 \cdot \sigma_2$, such that $\mathbf{rc}_r(\sigma_1) \wedge \sigma_2 \in \lceil \sigma_r \rceil$. Assume that the lemma holds for σ_1. Let $\sigma_1 \in \sigma_1'[r]$. From the definition of trace refinement it follows that $\sigma_2 \in a_r[r]$ and thus that $\sigma' \in (\sigma_1' \cdot a_r)[r]$, therefore $\sigma = \sigma_1' \cdot a_r$.

$q \xrightarrow{\lfloor \sigma_1 \cdot \sigma_2 \rfloor}_r q'$

$\Rightarrow$ $(*$ Definition $\longrightarrow$, $\sigma_2 \in \lceil \sigma_r \rceil$ does not start with δ $*)$

$\exists q_1 \in Q_r : q \xrightarrow{\lfloor \sigma_1 \rfloor}_r q_1 \xrightarrow{\lfloor \sigma_2 \rfloor}_r q'$

$\Rightarrow$ $(*$ Lemma A.15, note that $\mathbf{rc}_r(\sigma_1)$ $*)$

$\exists q_1 \in Q : q \xrightarrow{\lfloor \sigma_1 \rfloor}_r q_1 \xrightarrow{\lfloor \sigma_2 \rfloor}_r q'$

$\Rightarrow$ $(*$ Induction $*)$

$\exists q_1 \in Q : q \xrightarrow{\sigma_1'} q_1 \wedge q_1 \xrightarrow{\lfloor \sigma_2 \rfloor}_r q'$

$\Rightarrow$ $(*$ Lemma A.10 $*)$

$\exists q_1 \in Q : q \xrightarrow{\sigma_1'} q_1 \wedge q_1 \xrightarrow{a_r} q'$

$\Rightarrow$ $(*$ Definition $\longrightarrow$ $*)$

$q \xrightarrow{\sigma_1' \cdot a_r} q'$

$\Rightarrow$ $(*$ Definition trace refinement $(\sigma' = \sigma_1' \cdot a_r)$ $*)$

$q \xrightarrow{\sigma'} q'$

3. $\sigma' = \sigma_1 \cdot \lambda$, such that $\lambda \in L_r \backslash L(\sigma_r) \wedge \mathbf{rc}_r(\sigma_1) \wedge \nexists \sigma_2, \sigma_3 \in L_{r\delta}^* : \sigma = \sigma_1 \cdot \sigma_2 \wedge \sigma_2 \in \downarrow \lceil \sigma_r \rceil \backslash (\lceil \sigma_r \rceil \cup \{\epsilon\}$ and assume that the lemma holds for σ_1. Let $\sigma_1 \in \sigma_1'[r]$ this means that $\sigma' \in (\sigma_1' \cdot \lambda)[r]$ and thus that $\sigma = \sigma_1' \cdot \lambda$.

$q \xrightarrow{\lfloor \sigma_1 \cdot \lambda \rfloor}_r q'$

$\Rightarrow$ $(*$ Definition $\longrightarrow$ $*)$

$\exists q_1 \in Q_r : q \xrightarrow{\lfloor \sigma_1 \rfloor}_r q_1 \xrightarrow{\lambda}_r q'$

$\Rightarrow$ $(*$ Lemma A.15 $*)$

$\exists q_1 \in Q : q \xrightarrow{\lfloor \sigma_1 \rfloor}_r q_1 \xrightarrow{\lambda}_r q'$

$\Rightarrow$ $(*$ Induction $*)$

$\exists q_1 \in Q : q \xrightarrow{\sigma_1'} q_1 \wedge q_1 \xrightarrow{\lambda}_r q'$

$\Rightarrow$ $(*$ Lemma A.9 $*)$

$\exists q_1 \in Q : q \xrightarrow{\sigma_1'} q_1 \wedge q_1 \xrightarrow{\lambda} q'$

$\Rightarrow$ $(*$ Definition $\longrightarrow$ $*)$

$q \xrightarrow{\sigma_1' \cdot \lambda} q'$

$\Rightarrow$ $(*$ $\sigma = \sigma_1' \cdot \lambda$ $*)$

$q \xrightarrow{\sigma} q'$

4. $\sigma' = \sigma_1 \cdot \lambda$, such that $\lambda = \delta \wedge \mathbf{rc}_r(\sigma_1) \wedge \nexists \sigma_2, \sigma_3 \in L_{r\delta}^* : \sigma = \sigma_1 \cdot \sigma_2 \wedge \sigma_2 \in \downarrow \lceil \sigma_r \rceil \backslash (\lceil \sigma_r \rceil \cup \{\epsilon\}$ and assume that the lemma holds for σ_1. Let $\sigma_1 \in \sigma_1'[r]$ this means that $\sigma' \in (\sigma_1' \cdot \lambda)[r]$ and thus that $\sigma = \sigma_1' \cdot \lambda$.

$$
\begin{array}{ll}
 & q \xrightarrow{\lfloor \sigma_1 \cdot \lambda \rfloor}_r q' \\
\Rightarrow & (* \text{ Lemma A.2 } *) \\
 & q \xrightarrow{\sigma_1 \cdot \lambda}_r q' \\
\Rightarrow & (* \text{ Definition } \longrightarrow \ *) \\
 & \exists q_1 \in Q : q \xrightarrow{\sigma_1}_r q_1 \xrightarrow{\lambda} q' \\
\Rightarrow & (* \text{ Lemma A.2 } *) \\
 & \exists q_1 \in Q : q \xrightarrow{\lfloor \sigma_1 \rfloor}_r q_1 \xrightarrow{\lambda}_r q' \\
\Rightarrow & (* \text{ Induction } *) \\
 & \exists q_1 \in Q : q \xrightarrow{\sigma_1'} q_1 \wedge q_1 \xrightarrow{\lambda}_r q' \\
\Rightarrow & (* \text{ Lemma A.9 } *) \\
 & \exists q_1 \in Q : q \xrightarrow{\sigma_1'} q_1 \wedge q_1 \xrightarrow{\lambda} q' \\
\Rightarrow & (* \text{ Definition } \longrightarrow \ *) \\
 & q \xrightarrow{\sigma_1' \cdot \lambda} q' \\
\Rightarrow & (* \ \sigma = \sigma_1' \cdot \lambda \ *) \\
 & q \xrightarrow{\sigma} q'
\end{array}
$$

□

Lemma A.17 Let $t_r \in t[r]$, $t \in \mathcal{TEST}(I,U)$ a sound test case for a specification $s \in \mathcal{LTS}(I,U)$ and **uioco**.

$$t_r \xrightarrow{\sigma}_r \mathbf{fail}_{t_r} \Rightarrow \exists \sigma' \in Utraces(s[r]), x \in U_{r\delta} : \sigma' \cdot x = \sigma \wedge x \notin out(s[r] \textbf{ after } \sigma')$$

Proof We distinguish two cases:

1. $\mathbf{fail}_{t_r} \in Q$

$$
\begin{array}{ll}
 & t \xrightarrow{\sigma}_r \mathbf{fail}_{t_r} \\
\Rightarrow & (* \text{ Lemma A.15 } *) \\
 & t \xrightarrow{\sigma}_r \mathbf{fail}_{t_r} \wedge \mathbf{rc}_r(\sigma) \\
\Rightarrow & (* \text{ Definition r-complete } *) \\
 & t \xrightarrow{\sigma}_r \mathbf{fail}_{t_r} \wedge \exists \sigma' \in L_\delta^* : \sigma \in \sigma'[r] \\
\Rightarrow & (* \text{ Lemma A.16 } *) \\
 & \exists \sigma' \in L_\delta^* : t \xrightarrow{\sigma'} \mathbf{fail}_{t_r} \wedge \sigma \in \sigma'[r] \\
\Rightarrow & (* \text{ Lemma A.3 } *) \\
 & \exists \sigma_1 \in Utraces(s), x \in U_\delta : \sigma \in (\sigma_1 \cdot x)[r] \wedge x \notin out(s \textbf{ after } \sigma_1) \\
\Rightarrow & (* \text{ Lemma 5.4 } *) \\
 & \exists \sigma_1 \in Utraces(s), x \in U_\delta : \sigma \in (\sigma_1 \cdot x)[r] \\
 & \wedge \forall \sigma_1' \in \sigma_1[r] : x \notin out(s[r] \textbf{ after } \sigma_1') \\
\Rightarrow & (* \text{ Logical reasoning } *) \\
 & \exists \sigma_1' \in Utraces(s[r]), x \in U_\delta : \sigma = \sigma_1' \cdot x \wedge x \notin out(s[r] \textbf{ after } \sigma_1')
\end{array}
$$

2. $\mathbf{fail}_{t_r} \in Q_{t_r} \backslash Q$

   By definition of test case refinement new (fail) states can only be reached via a mini-test. New fail states are pairs, where the second state is a fail state of a mini-test; let $\mathbf{fail}_{t_r} = (q, q')$

$$
\begin{array}{ll}
 & t_r \xrightarrow{\sigma}_r (q, q') \\
\Rightarrow & (* \text{ Definition test case refinement } *) \\
 & \exists q_1 \in Q, \sigma_1, \sigma_2 \in L_{r\delta}^* : \sigma = \sigma_1 \cdot \sigma_2 \wedge \exists mt \in MT : mt \xrightarrow{\sigma_2} q' \\
 & \wedge t_r \xrightarrow{\sigma_1}_r q_1 \wedge q_1 \xrightarrow{a_r} q
\end{array}
$$

We split this proof in two parts for better readability. First we show that $\sigma_2 \in \sigma_r|_1 \cdot \delta^? \cdots \delta^? \cdot \sigma_r|_i \cdot U$ for some $1 \leq i < n = |\sigma_r|$. Then we show that $\sigma_1 \cdot \lceil \sigma_r \rceil \subseteq \mathit{Utraces}(s)[r]$. We end the proof by combining these two results.

(a) To be proven: $\exists \sigma_2' \in \sigma_r|_1 \cdot \delta^* \cdots \delta^* \cdot \sigma_r|_i, x \in U : \sigma_2 = \sigma_2' \cdot x$

$\exists mt \in MT : mt \xrightarrow{\sigma_2} q' \in \mathbf{fail}_{mt}$
$\Rightarrow$ ($*$ Equation (8) in Lemma A.8 $*$)
$\exists 1 \leq i < n = |\sigma_r| : \sigma_2 \in \sigma_r|_1 \cdot \delta^? \cdots \delta^? \cdot \sigma_r|_i \cdot U$
$\Rightarrow$ ($*$ Logical reasoning $*$)
$\exists \sigma_2' \in \sigma_r|_1 \cdot \delta^? \cdots \delta^? \cdot \sigma_r|_i, x \in U : \sigma_2 = \sigma_2' \cdot x$

(b) To be proven: $\sigma_1 \cdot \lceil \sigma_r \rceil \subseteq \mathit{Utraces}(s)[r]$

$t_r \xrightarrow{\sigma_1}_r q_1 \wedge q_1 \xrightarrow{a_r} q$
$\Rightarrow$ ($*$ Lemma A.15 $*$)
$t_r \xrightarrow{\sigma_1}_r q_1 \wedge q_1 \xrightarrow{a_r} q \wedge \mathbf{rc}_r(\sigma_1)$
$\Rightarrow$ ($*$ Definition r-completeness $*$)
$t_r \xrightarrow{\sigma_1}_r q_1 \wedge q_1 \xrightarrow{a_r} q \wedge \exists \sigma_1' \in L_\delta^* : \sigma_1 \in \sigma_1'[r]$
$\Rightarrow$ ($*$ Lemma A.16 $*$)
$\exists \sigma_1' \in L_\delta^* : \sigma_1 \in \sigma_1'[r] \wedge t \xrightarrow{\sigma_1'} q_1 \wedge q_1 \xrightarrow{a_r} q$
$\Rightarrow$ ($*$ Definition $\longrightarrow$ $*$)
$\exists \sigma_1' \in L_\delta^* : \sigma_1 \in \sigma_1'[r] \wedge t \xrightarrow{\sigma_1' \cdot a_r} q$
$\Rightarrow$ ($*$ t is conformance-trace safe wrt **uioco** and s $*$)
$\exists \sigma_1' \in L_\delta^* : \sigma_1 \in \sigma_1'[r] \wedge \sigma_1' \cdot a_r \in \mathit{Utraces}(s)$
$\Rightarrow$ ($*$ Definition test case refinement and $a_r[r] = \lceil \sigma_r \rceil$ $*$)
$\sigma_1 \cdot \lceil \sigma_r \rceil \subseteq \mathit{Utraces}(s)[r]$

When we combine 1) and 2) we obtain the following result:

$\exists \sigma_1 \in L_{r\delta}^*, \sigma_2' \in \sigma_r|_1 \cdot \delta^? \cdots \delta^? \cdot \sigma_r|_i, x \in U : \sigma = \sigma_1 \cdot \sigma_2' \cdot x$
$\wedge \sigma_1 \cdot \lceil \sigma_r \rceil \subseteq \mathit{Utraces}(s)[r]$
$\Rightarrow$ ($*$ Definition trace refinement $*$)
$\exists \sigma_1 \in L_{r\delta}^*, \sigma_2' \in \sigma_r|_1 \cdot \delta^? \cdots \delta^? \cdot \sigma_r|_i, x \in U : \sigma = \sigma_1 \cdot \sigma_2' \cdot x$
$\wedge \sigma_1 \cdot \sigma_2' \in \downarrow(\mathit{Utraces}(s)[r]) \setminus \mathit{Utraces}(s)[r]$
$\Rightarrow$ ($*$ Logical reasoning $*$)
$\exists \sigma' \in \downarrow(\mathit{Utraces}(s)[r]) \setminus \mathit{Utraces}(s)[r], x \in U : \sigma = \sigma' \cdot x$
$\Rightarrow$ ($*$ Lemma 5.5 $*$)
$\exists \sigma' \in \downarrow(\mathit{Utraces}(s)[r]) \setminus \mathit{Utraces}(s)[r], x \in U : \sigma = \sigma' \cdot x$
$\wedge x \notin \mathit{out}(s[r] \,\mathbf{after}\, \sigma')$
$\Rightarrow$ ($*$ Lemma 5.3 $*$)
$\exists \sigma' \in \mathit{Utraces}(s[r]), x \in U : \sigma = \sigma' \cdot x \wedge x \notin \mathit{out}(s[r] \,\mathbf{after}\, \sigma')$

□

Theorem 7.6 [Soundness] Let $s \in \mathcal{LTS}(I,U), t \in \mathcal{TEST}(I,U)$ and let t be conformance trace safe with respect to **uioco** and s

t is **sound** w.r.t. **uioco** and $s \Rightarrow t[r]$ is **sound** w.r.t. **uioco** and $s[r]$

Proof We immediately expand the definitions of soundness and **uioco**. Let $\sigma \in \mathit{Utraces}(s[r])$. As you can see we rewrote the proof obligation into an equivalent logical formula $((A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A))$.

$i \xrightarrow{\sigma} \wedge\, t_r \xrightarrow{\sigma}_r \mathbf{fail}_{t_r}$

$\Rightarrow$ $(*$ Lemma A.17, note premise t is **sound** $*)$

$\exists \sigma' \in Utraces(s[r]), x \in U_{r\delta} : i \xrightarrow{\sigma' \cdot x} \wedge\, x \notin out(s[r] \textbf{ after } \sigma')$

$\Rightarrow$ $(*$ Definition *out* and **after** $*)$

$\exists \sigma' \in Utraces(s[r]), x \in U_{r\delta} : x \in out(i \textbf{ after } \sigma) \wedge x \notin out(s \textbf{ after } \sigma)$

$\Rightarrow$ $(*$ Definition **uioco** $*)$

$i \not\textbf{uioco}\ s[r]$

□

Lemma A.18 Let $s \in \mathcal{LTS}(I,U), \sigma \in Utraces(s[r]), T \subseteq \mathcal{TEST}(I,U)$ be an exhaustive test suite with respect to **uioco** and $s[r]$ and r-cov(T,s).

$$x \notin out(s[r] \textbf{ after } \sigma) \Rightarrow \exists t_r \in T[r] : t_r \xrightarrow{\lfloor \sigma \rfloor \cdot x}_r \mathbf{fail}_{t_r}$$

Proof

- $\sigma \in Utraces(s)[r]$

  $x \notin out(s[r] \textbf{ after } \sigma)$

  $\Rightarrow$ $(*$ Lemma 5.4 $*)$

  $x \notin out(s \textbf{ after } \sigma\langle r \rangle)$

  $\Rightarrow$ $(*$ Exhaustiveness T $*)$

  $\exists t \in T : t \xrightarrow{\sigma\langle r \rangle \cdot x} \mathbf{fail}_t$

  $\Rightarrow$ $(*$ Lemma A.16 $*)$

  $\forall \sigma' \in \sigma\langle r \rangle[r], \exists t_r \in T[r] : t_r \xrightarrow{\lfloor \sigma' \rfloor \cdot x}_r \mathbf{fail}$

  $\Rightarrow$ $(*$ Proposition A.4 $*)$

  $\exists t_r \in T[r] : t_r \xrightarrow{\lfloor \sigma \rfloor \cdot x}_r \mathbf{fail}_{t_r}$

- $\sigma \in \downarrow(Utraces(s)[r]) \setminus Utraces(s)[r]$

$$
\begin{array}{ll}
 & x \notin out(s[r] \textbf{ after } \sigma) \\
\Rightarrow & (* \text{ Lemma 5.5 } *) \\
 & x \neq \delta \\
\Rightarrow & (* \text{ Lemma A.5 } *) \\
 & x \neq \delta \wedge \exists \sigma_1, \sigma_2, \sigma_3 \in L^*_{r\delta} : \sigma = \sigma_1{\cdot}\sigma_2 \wedge \sigma_2{\cdot}\sigma_3 \in \lceil \sigma_r \rceil \wedge \mathbf{rc}_r(\sigma_1) \\
 & \wedge \sigma_1{\cdot}\sigma_2{\cdot}\sigma_3 \in Utraces(s)[r] \\
\Rightarrow & (* \text{ Logical reasoning } \sigma_3 \neq \epsilon \ *) \\
 & x \neq \delta \wedge \exists \sigma_1, \sigma_2, \sigma_3 \in L^*_{r\delta} : \sigma = \sigma_1{\cdot}\sigma_2 \wedge \sigma_2{\cdot}\sigma_3 \in \lceil \sigma_r \rceil \\
 & \wedge \sigma_2 \in \downarrow\lceil \sigma_r \rceil \backslash (\lceil \sigma_r \rceil \cup \{\epsilon\}) \wedge \mathbf{rc}_r(\sigma_1) \wedge \sigma_1{\cdot}\sigma_2{\cdot}\sigma_3 \in Utraces(s)[r] \\
\Rightarrow & (* \text{ Definition trace contraction } *) \\
 & x \neq \delta \wedge \exists \sigma_1, \sigma_2 \in L^*_{r\delta} : \sigma = \sigma_1{\cdot}\sigma_2 \wedge \sigma_2 \in \downarrow\lceil \sigma_r \rceil \backslash (\lceil \sigma_r \rceil \cup \{\epsilon\}) \\
 & \wedge \mathbf{rc}_r(\sigma_1) \wedge \sigma_1\langle r \rangle{\cdot}a_r \in Utraces(s) \\
\Rightarrow & (* \ r\text{-cov}(T, s) \ *) \\
 & x \neq \delta \wedge \exists \sigma_1, \sigma_2 \in L^*_{r\delta} : \sigma = \sigma_1{\cdot}\sigma_2 \wedge \sigma_2 \in \downarrow\lceil \sigma_r \rceil \backslash (\lceil \sigma_r \rceil \cup \{\epsilon\}) \\
 & \wedge \mathbf{rc}_r(\sigma_1) \wedge \exists t \in T : t \xrightarrow{\sigma_1\langle r \rangle{\cdot}a_r} \\
\Rightarrow & (* \text{ Lemma A.13 } *) \\
 & x \neq \delta \wedge \exists \sigma_1, \sigma_2 \in L^*_{r\delta} : \sigma = \sigma_1{\cdot}\sigma_2 \wedge \sigma_2 \in \downarrow\lceil \sigma_r \rceil \backslash (\lceil \sigma_r \rceil \cup \{\epsilon\}) \\
 & \wedge \mathbf{rc}_r(\sigma_1) \wedge \forall \sigma_1' \in \sigma_1\langle r \rangle[r], \sigma_2' \in \downarrow\lceil \sigma_r \rceil \backslash (\lceil \sigma_r \rceil \cup \{\epsilon\}, y \in U, \\
 & \exists t_r \in T[r] : t_r \xrightarrow{\lfloor \sigma_1'{\cdot}\sigma_2' \rfloor{\cdot}y}_r \mathbf{fail}_{t_r} \\
\Rightarrow & (* \text{ Proposition A.4 } *) \\
 & x \neq \delta \wedge \exists \sigma_1, \sigma_2 \in L^*_{r\delta} : \sigma = \sigma_1{\cdot}\sigma_2 \wedge \sigma_2 \in \downarrow\lceil \sigma_r \rceil \backslash (\lceil \sigma_r \rceil \cup \{\epsilon\}) \\
 & \wedge \mathbf{rc}_r(\sigma_1) \wedge \forall \sigma_2' \in \downarrow\lceil \sigma_r \rceil \backslash (\lceil \sigma_r \rceil \cup \{\epsilon\}, y \in U, \\
 & \exists t_r \in T[r] : t_r \xrightarrow{\lfloor \sigma_1{\cdot}\sigma_2' \rfloor{\cdot}y}_r \mathbf{fail}_{t_r} \\
\Rightarrow & (* \text{ Logical reasoning } *) \\
 & \exists t_r \in T[r] : t_r \xrightarrow{\lfloor \sigma \rfloor{\cdot}x}_r \mathbf{fail}_{t_r}
\end{array}
$$

□

Theorem 7.8 [Exhaustiveness] Let $s \in \mathcal{LTS}(I,U), T \subseteq \mathcal{TEST}(I,U), r\text{-cov}(T,s)$ T is **exhaustive** w.r.t. **uioco** and $s \Rightarrow T[r]$ is **exhaustive** w.r.t. **uioco** and $s[r]$

Proof We immediately expand the definitions of exhaustiveness and **uioco**. Let $\sigma \in Utraces(s[r])$.

$$
\begin{array}{ll}
 & x \in out(i \textbf{ after } \sigma) \wedge x \notin out(s[r] \textbf{ after } \sigma) \\
\Rightarrow & (* \text{ Lemma A.7 } *) \\
 & x \in out(i \textbf{ after } \lfloor \sigma \rfloor) \wedge x \notin out(s[r] \textbf{ after } \lfloor \sigma \rfloor) \\
\Rightarrow & (* \text{ Lemma A.18 } *) \\
 & x \in out(i \textbf{ after } \lfloor \sigma \rfloor) \wedge \exists t_r \in T[r] : t_r \xrightarrow{\lfloor \sigma \rfloor{\cdot}x}_r \mathbf{fail} \\
\Rightarrow & (* \text{ Definition } out \text{ and } \textbf{after } *) \\
 & i \xRightarrow{\lfloor \sigma \rfloor{\cdot}x} \wedge \exists t_r \in T[r] : t_r \xrightarrow{\lfloor \sigma \rfloor{\cdot}x}_r \mathbf{fail}
\end{array}
$$

□

References

[1] G. Bernot, M. G. Gaudel, and B. Marre. Software testing based on formal specifications: a theory and a tool. *Software Engineering Journal*, 1991(November):387–405, 1991. Also: Rapport de Recherche 581, L.R.I., Université de Paris-Sud.

[2] R. Gorrieri and A. Rensink. Action refinement. In J. A. Bergstra, A. Ponse, and S. A. Smolka, editors, *Handbook of Process Algebra*, chapter 16, pages 1047–1147. Elsevier, 2001.

[3] A. Petrenko, G. v. Bochmann, and R. Dssouli. Conformance relations and test derivation. In O. Rafiq, editor, *Sixth Int. Workshop on Protocol Test Systems*, number C-19 in IFIP Transactions, pages 157–178. North-Holland, 1994.

[4] J. Tretmans. Test generation with inputs, outputs, and quiescence. In T. Margaria and B. Steffen, editors, *Second Int. Workshop on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'96)*, pages 127–146. Lecture Notes in Computer Science 1055, Springer-Verlag, 1996.

[5] J. Tretmans. Test generation with inputs, outputs and repetitive quiescence. *Software—Concepts and Tools*, 17(3):103–120, 1996.

[6] M. van der Bijl, A. Rensink, and J. Tretmans. Action refinement in conformance testing. CTIT Technical Report TR–CTIT–05–10, University of Twente, Feb. 2004. URL: http://www.ub.utwente.nl/webdocs/ctit/1/00000123.pdf.

[7] M. van der Bijl, A. Rensink, and J. Tretmans. Action refinement roadmap, 2004. URL: http://wwwhome.cs.utwente.nl/~vdbijl/papers.

[8] M. van der Bijl, A. Rensink, and J. Tretmans. Compositional testing with ioco. In A. Petrenko and A. Ulrich, editors, *FATES 2003*, volume 2931 of *Lecture Notes in Computer Science*, pages 86–100. Springer, 2004.