

Formal Test Purposes and the Validity of Test Cases

Peter H. Deussen¹ and Stephan Tobies²

¹ Fraunhofer FOKUS, Berlin, Germany, deussen@fokus.fhg.de

² Nokia Research Center, Bochum, Germany, Stephan.Tobies@nokia.com

Abstract. We give a formalization of the notion of test purpose based on (suitably restricted) Message Sequence Charts. We define the validity of test cases with respect to such a formal test purpose and provide a simple decision procedure for validity.

1 Introduction

The quality of a test system directly influences the quality of the tested implementation: high quality test systems are essential to obtain high quality implementations. Hence, a common problem in the testing area is the so-called “test the tester” problem [12]: how can the validity of a test system with respect to a given specification, and therefore the quality of the test system, be assured? To put it in conformance testing terminology: how can it be assured that a test case achieves its test purpose?

One approach used to obtain valid test systems is the derivation of test cases from formal specifications or test purpose definitions. Other approaches focus on the manual or automated simulation against a formal specification (see [14] for a description of tools that employ these two approaches). While many modern telecommunication protocols come with (semi-) formal specifications of test purposes, a formal protocol description is provided only in very few cases (see [5] for a notable exception). For example, Internet Protocols defined in RFCs use natural language to define the semantics of the specification. Due to this, a formal description of the specification would have to be elaborated to allow for an automatic generation of valid test cases. Additionally, even if formal descriptions are available, automated generation methods only generate test skeletons that need to be manually refined to obtain executable test cases for the execution against a concrete system implementation. For all these reasons, the implementation of test cases is still performed mainly in a manual manner.

In this paper, we give a new answer to the “test the tester problem”, namely, to check the validity of a (possibly hand-written) test case against a formal test purpose definition. It does not rely on the existence of a formal description of the system under test (SUT) or the test system, but requires a formally defined test purpose. From this test purpose, the allowed and required behavior of the test case is derived. This information is then used in a guided simulation of the executable test system to determine whether the test system is valid with respect to this test purpose. Since our approach is solely based on test purposes, it is not necessary to develop a complete formal specification of the system as test purposes are only a partial description of the system. We use Message Sequence Charts (MSC) as the formal test purpose description language [6], which is

widely used in the system development process in the telecommunication area. This allows for an easy re-use of the uses-cases developed during system design as a solid basis for the test purpose definition. This further reduces the work necessary for the test purpose specification.

Despite the fact that MSCs are widely used to capture test purpose, theoretical studies of MSCs so far seem to have failed to address the following issues:

- What does it mean for a test case to implement a test purpose, i.e., when is a test case *valid* w. r. t. a test purpose?
- When is an MSC a *well-formed* test purpose, i. e., when does an MSC characterize behavior that is indeed (black-box) testable?

We address these issues using a semantics for MSC based on pomsets [11,4] in the spirit of [8]. We then describe a simple decision procedure for the validity of test cases w. r. t. a test purpose and prove its correctness.

The paper is structured as follows: Section 2 of this paper introduces the partial order semantics of MSCs and their usage as formal test purposes. In Section 3, we define test case validity, describe the decision procedure and prove its correctness. Section 4 presents one possible implementation design for an MSC based test validator. Section 4 concludes. Proofs of key lemmata and theorems can be found in the appendix.

2 Formal Test Purposes

To check (or even define) validity of a test case wrt. a test purposes, we need a formal definition of a test purpose together with suitable semantics. In this section, we suggest a formalism to formally express test purposes and establish a set of criteria that guarantee that a test purposes indeed describes (black-box) testable behavior.

We use Message Sequence Charts (MSCs) to express formal test purposes because they are widely used to capture test purposes and semantics based on different approaches are available. We have chosen semantics based on pomsets [4,11] in an adaption of the definition of [8] to better suit our purposes. The particular choice of semantics of MSCs is not central to our approach, but obviously some choice has to be made. Using the more operational semantics from [9,7] would lead to similar results.

After a short overview on the employed MSC syntax for test purposes, we recapitulate the pomset-based semantics of MSC and define when an MSC constitutes as well-formed test purpose.

Message Sequence Charts. The MSCs in Fig. 1 serves as an explanatory example for the basic MSC language as used throughout this paper. The most fundamental constructs of MSCs are *instances* and *messages*. Instances represent components or communication interfaces that exhibit a sequential behaviour. Our example MSC m_1 consists of three instances p , q , and r . A message exchange between a sending instance p and a receiving instance q comprises two *events* $!_{p,q}a$ and $?_{p,q}a$ for sending the message a at p and for receiving a at q , respectively. Graphically, messages are depicted by arrows between instances labeled with messages.

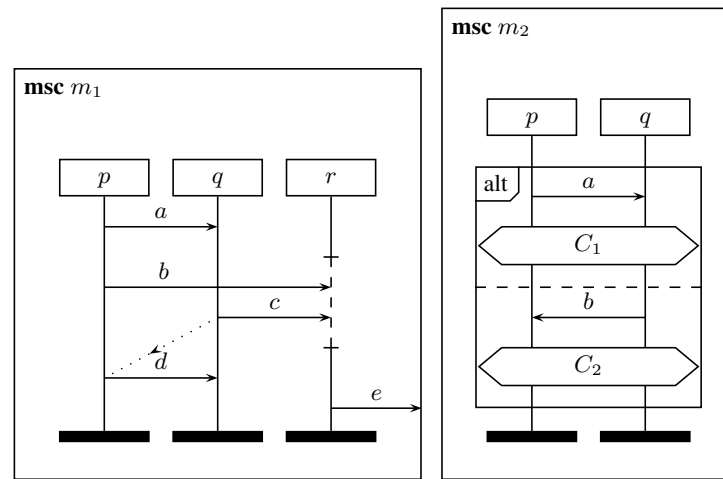


Fig. 1. Example MSCs.

Events are considered to be causally or temporally ordered only if they are located at the same instance (in this case the ordering is top-to-bottom), or if they are part of the same message exchange. In our example m_1 , the event $!_{p,q}a$ precedes the events $?_{p,q}a$ and $!_{p,r}b$, but no assumption on an ordering of the events $!_{p,r}b$ and $!_{q,r}c$ is expressed, even if $!_{p,r}b$ is drawn above $!_{q,r}c$.

There is a way to express the concurrency of events of the same instance: the concurrent region (*coregion*, for short). Coregions are depicted by dashed sections on the corresponding instance line bordered by small horizontal bars: the events that occur on this dashed section are supposed to happen in parallel. In our example, the events $?_{p,r}b$ and $?_{q,r}c$ are temporally unrelated. On the other hand, it is possible to use *general order* arrows (dotted lines between events with an arrow head in their middle section) to express causal orderings of events on different instances. In m_1 , the event $!_{q,r}c$ precedes $!_{p,q}d$. Finally, the MSC language allows to express message exchange with the environment of a MSC; e. g. in m_1 the message e is send to the environment of this MSC.

The MSC formalism provides not only communication primitives but also control structures. For our purposes, only the *alt operator*, modeling nondeterministic choice, is of importance. m_2 in Fig. 1 shows an example: A choice between sending a from p to q and sending b from q to p is expressed. A final construct considered in this paper is that of *conditions*. Conditions model global states or predicates related to more than on instance; m_2 contains two conditions C_1 and C_2 . It is not an easy task to assign a formal meaning to conditions. However, we use conditions only to express test verdicts and handle them formally in a special way. We will discuss this topic in detail in a later section.

Other important concepts of the basic MSC language not covered in this paper are: *loop inline expressions* (since tests are finite, loops occurring in test purposes comprises always finite, fixed boundaries and therefore can be unfolded), and especially *timers*, which require extra considerations and will be dealt with in forthcoming work.

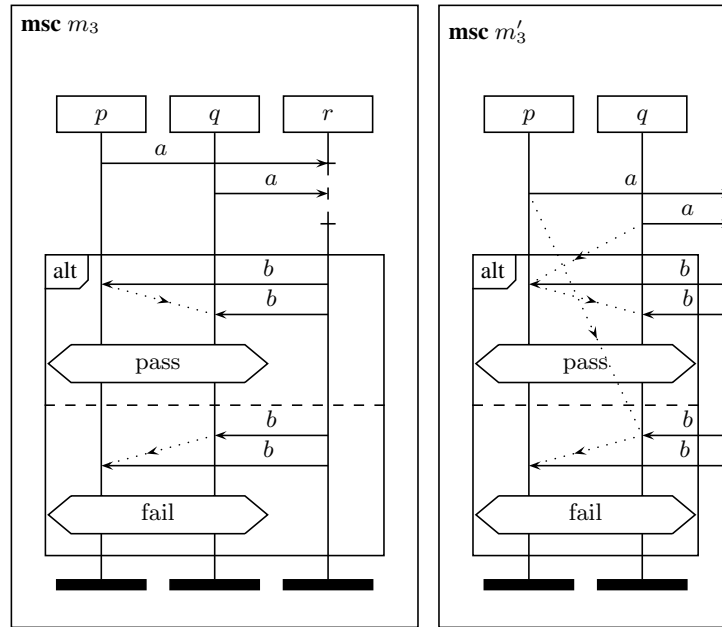


Fig. 2. Expressing the same test purposes with and without SUT instances

Expressing test purposes. We will use the MSC formalism to capture test purposes in the following way: the set of instances is partitioned into a non-empty set of port instances and a non-empty set of SUT instance. Intuitively, the port instances represent the different ports (PCOs, interfaces) at which the SUT interacts with its environment. Conditions that span the port instances are used to assign the test verdicts.

The SUT instances are used as “syntactic sugar” and serve two purposes: (1) as communication partners for the port instances, and (2) to impose an ordering of the sequence of messages. The same could be achieved by using communication with the environment and generalized orderings, but our approach leads to a more concise and intuitive representation of the test purpose and matches the common usage. Fig. 2 shows the two alternative ways of depicting a simple test purpose: after having received the message a on both its ports p and q (in arbitrary order), the SUT answers by sending the message b , again both on port p and q . If the message is sent on port p before it is sent on port q then the SUT shall pass the test, otherwise it shall fail. We will come back to this example later in this paper.

2.1 Partial Orders

We quickly recapitulate how pomsets can be used to assign a semantics to MSCs. We start by introducing the basic notations used throughout this paper.

To avoid tedious notation, we fix the following convention: if a structure $S = \langle A, B, \dots \rangle$ is introduced, the components of S will be denoted by A_S, B_S, \dots

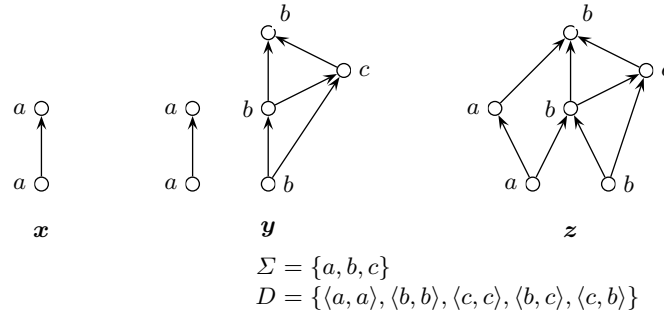


Fig. 3. Example pomsets

For some set A , $\mathcal{P}(A)$ is the set of all subsets of A . For $R \subseteq A \times B$ and $a \in A$, we denote the *image* of a under R by $R(a) =_{\text{df}} \{b \in B : a R b\}$. For $C \subseteq A$ we define $R(C) =_{\text{df}} \bigcup_{a \in C} R(a)$. The *inverse* R^{-1} of a relation R , the identity relation id_A on A , the relational composition $R \cdot S$ or two relations R, S , the transitive closure R^+ of R , and the reflexive-transitive closure R^* of R are defined in the usual manner.

Lposets. For the rest of this paper let us fix a finite alphabet Σ . A *labeled partial order* (lposet, for short) over Σ is a structure $x = \langle E, <, \lambda \rangle$ where E is a finite set of *events*, $< \subseteq E \times E$ is an (irreflexive) partial order, and $\lambda : E \rightarrow \Sigma$ is a labeling function.

Let x be a lposet and let $e_1, e_2 \in E_x$. We use the following notions: The *reflexive closure* of $<_x$ is $\leq_x =_{\text{df}} <_x \cup \text{id}_{E_x}$. Unrelated events are called *concurrent*, i. e., $e_1 \text{ co}_x e_2 \Leftrightarrow_{\text{df}} e_1 \not\leq_x e_2 \ \& \ e_2 \not\leq_x e_1$, while related events are *in line*: $e_1 \text{ li}_x e_2 \Leftrightarrow_{\text{df}} e_1 <_x e_2 \vee e_2 <_x e_1$. The *downward closure* of a set $D \subseteq E_x$ is $\downarrow_x D =_{\text{df}} \leq_x^{-1}(D)$. If $D = \downarrow_x D$ holds, then D is called *downward closed* in x . By $\mathbf{C}(x)$ we denote the set of downward closed sets in x . If $D \subseteq E_x$, then $x[D] =_{\text{df}} \langle D, <_x \cap (D \times D), \lambda \upharpoonright D \rangle$ is the lposet *generated by* D in x ($\lambda \upharpoonright D$ denotes the restriction of λ to D).

Pomsets. Lposets x and y over Σ are called *isomorphic*, written $x \equiv y$, if there is a bijection $f : E_x \rightarrow E_y$ such that $(e_1 <_x e_2 \Leftrightarrow f(e_1) <_y f(e_2)) \ \& \ \lambda_x = \lambda_y \circ f$ holds. A *partially ordered multiset* (a *pomset* for short) over Σ is an isomorphism class of lposets, i. e., a set $[x] =_{\text{df}} \{y : x \equiv y\}$. We fix the convention, that pomsets are denoted by boldfaced small letters $\mathbf{x}, \mathbf{y}, \mathbf{z}$. Moreover \mathbf{x} is assumed to be the equivalence class $[x]$ of x . By this convention, E_x always denotes the set of events of a representative x of \mathbf{x} . The class of pomsets over Σ is denoted by $\mathbf{P}(\Sigma)$.

Fig. 3 shows examples of pomsets. Graphically, we represent pomsets as directed acyclic (not necessarily connected) graphs. Nodes are labeled with elements from the underlying alphabet Σ . Transitive arcs are sometimes omitted.

Let $\mathbf{x}, \mathbf{y} \in \mathbf{P}(\Sigma)$ be pomsets. Then \mathbf{x} is called a *prefix* of \mathbf{y} —denoted $\mathbf{x} \leq \mathbf{y}$ —iff there are representatives $x \in \mathbf{x}$ and $y \in \mathbf{y}$ such that $E_x \subseteq E_y \ \& \ \mathbf{C}(x) \subseteq \mathbf{C}(y)$ holds. If there are representatives $x \in \mathbf{x}$ and $y \in \mathbf{y}$ such that $E_x = E_y \ \& \ <_x \subseteq <_y$ holds, then \mathbf{x} is called *less sequential* than \mathbf{y} . This is denoted by $\mathbf{x} \preceq \mathbf{y}$. It is easy to see that both \leq and \preceq partially order $\mathbf{P}(\Sigma)$. In Fig. 3, $\mathbf{x} \leq \mathbf{y}$, $\mathbf{x} \leq \mathbf{z}$, and $\mathbf{y} \preceq \mathbf{z}$, holds.

An alternative definition of the prefix relation \leq and the ordering by the degree of sequentiality \preceq can be obtained by introducing the notion of *weak homomorphisms* between representatives of pomsets [2].

Special pomsets that will be encountered in this paper are:

1. Letters $a = [\{a\}, \emptyset, a \mapsto a]$ for $a \in \Sigma$ (we abuse a, b, c, \dots to denote both letters from $\mathbf{P}(\Sigma)$ and from Σ).
2. Strings $[\{0, \dots, n-1\}, <, i \mapsto a_i]$ for $a_0 a_1 \dots a_{n-1} \in \Sigma^*$, where $<$ denotes the standard order relation on integers.
3. The empty word $\varepsilon = [\emptyset, \emptyset, \emptyset]$.

In this paper we do not distinguish between strings and pomset strings, i. e. if Σ is an alphabet then Σ^* is considered to be the set of pomsets σ over Σ such that $<_\sigma$ is a total ordering. If $\mathbf{x} \in \mathbf{P}(\Sigma)$, then by $\text{lin}(\mathbf{x}) =_{\text{df}} \{\sigma \in \Sigma^* : \mathbf{x} \preceq \sigma\}$ we denote the set of *linearizations* of \mathbf{x} .

Dependencies and Weak Sequential Composition. A reflexive and symmetric relation $D \subseteq \Sigma \times \Sigma$ is called a *dependence* on Σ ; for the rest of this paper let D be a dependence on Σ . If \mathbf{x} and \mathbf{y} are lposets over Σ , such that $E_{\mathbf{x}} \cap E_{\mathbf{y}} = \emptyset$ holds, then the *weak sequential composition* $\mathbf{x} \circ_D \mathbf{y}$ is defined by

$$\mathbf{x} \circ_D \mathbf{y} =_{\text{df}} [E_{\mathbf{x}} \cup E_{\mathbf{y}}, (<_{\mathbf{x}} \cup <_{\mathbf{y}} \cup R)^+, \lambda_{\mathbf{x}} \cup \lambda_{\mathbf{y}}],$$

where $R \subseteq E_{\mathbf{x}} \times E_{\mathbf{y}}$ is given by $e_1 R e_2 \Leftrightarrow_{\text{df}} \lambda_{\mathbf{x}}(e_1) D \lambda_{\mathbf{y}}(e_2)$.

A pomset \mathbf{x} is called *D-consistent* if we have, for all $e_1, e_2 \in E_{\mathbf{x}}$, $e_1 \text{ co}_x e_2 \Rightarrow \neg \lambda_{\mathbf{x}}(e_1) D \lambda_{\mathbf{x}}(e_2)$. Let $\mathbf{P}(\Sigma, D)$ denote the class of *D-consistent* pomsets. Clearly, if \mathbf{x} and \mathbf{y} are *D-consistent*, then also $\mathbf{x} \circ_D \mathbf{y}$ is.

Another operation on pomsets which is closely related to \circ_D is the *unsequentialization* via D : If $\mathbf{x} \in \mathbf{P}(\Sigma)$, then by $\langle \mathbf{x} \rangle_D$ we denote the pomset $[E_{\mathbf{x}}, R^+, \lambda_{\mathbf{x}}]$, where $R \subseteq E_{\mathbf{x}} \times E_{\mathbf{x}}$ is defined by $e_1 R e_2 \Leftrightarrow_{\text{df}} e_1 \leq e_2 \ \& \ \lambda_{\mathbf{x}}(e_1) D \lambda_{\mathbf{x}}(e_2)$.¹

The pomsets in Fig. 3 are all *D-consistent* for the dependence D shown in that figure. We have $\langle \mathbf{z} \rangle_D = \mathbf{y}$.

The following lemma justifies the relation between the operations \circ_D and $\langle \cdot \rangle_D$.

Lemma 1. *Let \mathbf{x}, \mathbf{y} in $\mathbf{P}(\Sigma)$. Then $\langle \mathbf{x} \circ_D \mathbf{y} \rangle_D = \langle \mathbf{x} \rangle_D \circ_D \langle \mathbf{y} \rangle_D$.*

Some more definitions: if $A \subseteq \Sigma$ is a set of symbols and \mathbf{x} is a pomset, then $\mathbf{x} \upharpoonright A =_{\text{df}} [x[\lambda_{\mathbf{x}}^{-1}(A)]]$. $\mathbf{x} \upharpoonright A$ is called the *restriction of \mathbf{x} to A* , i.e., \mathbf{x} restricted to those events labeled with elements from A . Finally, a set of pomsets $X \subseteq \mathbf{P}(\Sigma)$ is called *pre-closed* if $\mathbf{x} \in X \ \& \ \mathbf{y} \leq \mathbf{x} \Rightarrow \mathbf{y} \in X$ holds.

2.2 Partial Order Semantics for MSCs

To define the semantics of MSCs based on pomsets, we first need to fix an alphabet Σ_c and a dependence D_c on Σ_c .

¹ The operations \circ_D and $\langle \cdot \rangle_D$ impose an interesting and fruitful connection to the theory of Mazurkiewicz traces [10]. Although it is far beyond the scope of this paper it should be noted that pomsets of the form $\langle \mathbf{x} \rangle_D \in \mathbf{P}(\Sigma, D)$ are just alternative representations of Mazurkiewicz traces: in fact we have that $\text{lin}(\langle \mathbf{x} \rangle_D)$ is a Mazurkiewicz trace over Σ and D ; moreover, the operation \circ_D coincides with trace concatenation.

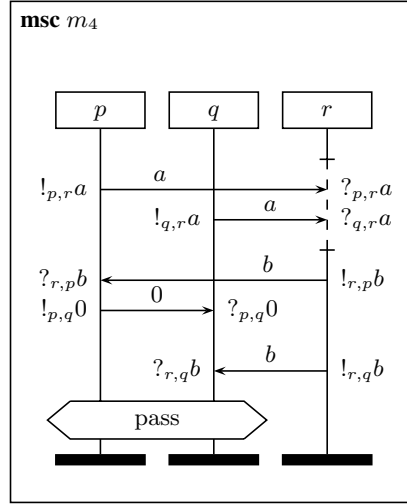


Fig. 4. An annotated MSC.

Communication Alphabet and Dependence. Let M be a set of *messages* and P a set of *instances* fixed throughout this paper. We assume that there is a non-empty set $T \subset P$ of *port instances*; the instances in $P - T$ will be called *SUT instances*. Usually we will have $|P - T| = 1$, but the theory presented in the following does not rely on this.

Let $\Sigma_!$, $\Sigma_?$ be the two alphabets:

1. $\Sigma_! =_{\text{df}} \{!\} \times P \times M \times P$ is the set of *send actions*. Its elements $\langle !, p, m, q \rangle$ will be denoted by $!_{p,q}m$,
2. $\Sigma_? =_{\text{df}} \{?\} \times P \times M \times P$ is the set of *receive actions*. Its elements $\langle ?, p, m, q \rangle \in \Sigma_?$ will be denoted by $?_{p,q}m$.

We put $\Sigma_c =_{\text{df}} \Sigma_! \cup \Sigma_?$ to be the set of *communications*. The mapping $\iota_c(a)$ identifies the *instance* of an action $a \in \Sigma_c$, i. e., $\iota_c(!_{p,q}m) =_{\text{df}} p$ and $\iota_c(?_{p,q}m) =_{\text{df}} q$. We put $\Sigma_o =_{\text{df}} \{a \in \Sigma_c : \iota_c(a) \in T\}$ to be the set of *tester observable actions*. For convenience, we furthermore define $\Sigma_o^! =_{\text{df}} \Sigma_o \cap \Sigma_!$ and $\Sigma_o^? =_{\text{df}} \Sigma_o \cap \Sigma_?$.

Fig. 4 gives a few examples of this syntax of actions. It shows the expansion of the first alternative of m_4 where the generalized ordering has been replaced by sending the void message 0. The messages have been annotated with the corresponding symbols from Σ_c .

To build pomsets from actions, we define the dependence D_c on Σ_c : let $D_c \subseteq \Sigma_c \times \Sigma_c$ be the smallest reflexive, symmetric relation containing:

- $\langle a, b \rangle$ with $\iota_c(a) = \iota_c(b)$ and a and b are not placed on the same co-region,
- $\langle !_{p,q}m, ?_{p,q}m \rangle$ for instances $p, q \in P$ and messages $m \in M$.

To keep things simple, we restrict ourself to the following MSC operators: message sending and receiving, co-regions, and the alternative inline expression, which allows the expression of optional behavior and finite iterations. We simulate general ordering by sending a void message 0, which might also be sent between two port or SUT instances.

Conditions are only allowed to assign verdicts and are not dealt with by the semantics. In order to obtain a set of D_c -consistent pomsets, we have to impose the restriction that identical actions (e. g. sending of a message twice from an instance p to an instance q) are not placed on the same co-region.

The semantics of an MSC \mathcal{M} is given by a pre-closed set of pomsets $X_{\mathcal{M}} \subseteq \mathbf{P}(\Sigma_c, D_c)$. We illustrate the construction of $X_{\mathcal{M}}$ only by informal means of an example (m_3 from Fig. 2); the translation is done similar to [8] with slightly different syntax for events of pomsets.

In the following, \circ_c abbreviates \circ_{D_c} .

The semantics of our example m_3 is given by the set X_{m_3} :

$$X_{m_3} = \{z \in \mathbf{P}(\Sigma_c, D_c) : z \leq x \circ_c y_1 \vee z \leq x \circ_c y_2\}.$$

where x , y_1 , and y_2 are defined by:

$$x =_{\text{df}} !_{p,r}a \circ_c !_{q,r}a \circ_c ?_{p,r}a \circ_c ?_{q,r}a \quad (1)$$

$$y_1 =_{\text{df}} !_{r,p}b \circ_c ?_{r,p}b \circ_c !_{p,q}0 \circ_c ?_{p,q}0 \circ_c !_{r,q}b \circ_c ?_{r,q}b \quad (2)$$

$$y_2 =_{\text{df}} !_{r,q}b \circ_c ?_{r,q}b \circ_c !_{q,p}0 \circ_c ?_{q,p}0 \circ_c !_{r,p}b \circ_c ?_{r,p}b \quad (3)$$

Without a proof (which would require a more formal treatment of the definition of $X_{\mathcal{M}}$ we state:

Lemma 2. *If \mathcal{M} is a MSC, then $\langle x \rangle_{D_c} = x$ for all $x \in X_{\mathcal{M}}$.*

2.3 Message Sequence Charts as Test Purposes

Now that we have explained how to assign semantics to an MSC, we show how MSCs can be utilized as a formal language to express test purposes. We discuss how the notion of a test verdict can be integrated into an MSC and how it can be guaranteed that an MSC specifies behavior that is amenable to black-box testing.

Verdict assignments. Syntactically, a verdict assignment is expressed by a condition on the port instances on the very end of each terminal alternative of the MSC. Semantically, the condition-like constructs pass, fail, and inconc are not treated as an ordinary condition but as a convenient way to define a *verdict assignment*:²

Let $V =_{\text{df}} \{\text{pass}, \text{fail}, \text{inconc}, \text{none}\}$ be a set of *verdicts* and let $V_f =_{\text{df}} V - \{\text{none}\}$ be the set of *final verdicts*. A mapping $v : X \rightarrow V$ for some finite, pre-closed set of pomsets X is called a *verdict assignment* to X if, for all $x \in X$, we have:

1. $\exists y \in X. x \leq y \ \& \ v(y) \neq \text{none}$, i. e., every pomset can be extended to a pomset that is assigned a final verdict, and
2. $v(x) \neq \text{none} \Rightarrow \forall y \in X. x \not\prec y$, i. e., pomsets that are assigned a final verdict are maximal in X .

² Alternatively, one could allow verdict conditions to appear also at other places within the MSC and, e. g., use the verdict assignment rules of TTCN-3 [3] to resolve the case where different verdicts are encountered during a single run through the MSC.

The verdict conditions drawn in an MSC \mathcal{M} are used to define a verdict mapping $v_{\mathcal{M}}$. Again, we introduce this informally by the example of m_3 from Fig. 2, where v_{m_3} is defined by:

$$v_{m_3}(z) = \begin{cases} \text{pass,} & \text{if } z = x \circ_c y_1; \\ \text{fail,} & \text{if } z = x \circ_c y_2; \\ \text{none,} & \text{otherwise.} \end{cases}$$

It is obvious that not every MSC that satisfies the syntactic restrictions that have been introduced above constitutes a test purpose, i. e., describes behavior of the SUT that can be tested in a black box testing approach. For example consider a modification of m_3 from Fig. 2, where the generalized ordering constraints have been eliminated. There the verdict does not depend on the order in which the messages b can be observed at the ports of the SUT but rather on the (SUT-internal) events that cause these messages to be sent. Clearly, such an event is not visible to a black-box test system and hence no test case can distinguish between the behavior of the first and second alternative. In the following we present a number of criteria that an MSC must satisfy to be considered a *well-formed* test purpose. Later we will see that these criteria indeed guarantee the existence of a valid test case for a test purpose.

Well-Formed Test Purposes. First, we define a function that reduces the semantics of an MSC to the information that is available to the test case, i. e., the sequences of events that occur on port instances:

Given test purpose MSC \mathcal{M} with semantics $X_{\mathcal{M}}$. For $x \in X_{\mathcal{M}}$, we define the *tester observable traces* of x by $\text{obs}(x) =_{\text{df}} \text{lin}(x \upharpoonright \Sigma_o)$.

A MSC \mathcal{M} is called a *well-formed test purpose* if it is possible to determine its state (and hence assigned verdict) based on this information in its tester observable traces, i. e., if

WF₁. for every $x, y \in X_{\mathcal{M}} \upharpoonright \Sigma_o$, $\text{lin}(x) \cap \text{lin}(y) \neq \emptyset$ implies $x = y$.

Unfortunately, this restriction does not yet suffice to guarantee that an MSC describes testable behavior. Another aspect that needs considerations is which party resolves *essential choice* in the sense of the following definition:

Let $X \subseteq \mathbf{P}(\Sigma_c, D_c)$ be a pre-closed set of pomsets. A pomset $x \in X$ is called a *choice point* for two actions $a, b \in \Sigma_c$ in X if $x \circ_c a \in X$, $x \circ_c b \in X$, and

$$\{y \in \max_{\leq}(X) : x \circ_c a \leq y\} \neq \{y \in \max_{\leq}(X) : x \circ_c b \leq y\},$$

where $\max_{\leq}(X)$ denotes the \leq -maximal pomsets in X .

Coming back to example from Fig. 2 with semantics X_{m_3} as defined in (1)– (3), $x \upharpoonright \Sigma_o$ is a choice point for $?_{r,p}b$ and $?_{r,q}b$. On the other hand, ε is not a choice point even though there are two “available” communications, namely $!_{p,r}a$ and $!_{q,r}a$, since this choice does not alter the reachable maximal configurations.

We require, for a well-formed test purpose, that each choice point is resolved by a message from the SUT:

WF₂. If x is a choice point of $X_{\mathcal{M}} \upharpoonright \Sigma_o$ for actions $a, b \in \Sigma_o$, then both $a, b \in \Sigma_o^?$.

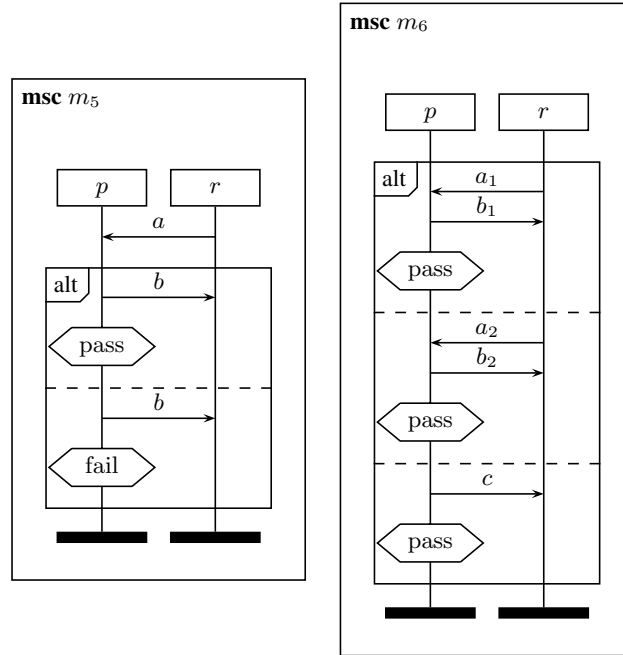


Fig. 5. Two malformed MSCs

This restriction is necessary because both other possibilities for a choice point ($a, b \in \Sigma_o^!$ or $a \in \Sigma_o^!$ and $b \in \Sigma_o^?$) are undesirable in a test purpose: a choice that has to be resolved by the test case indicates that the test purpose should indeed be (at least) two test purposes, one for each choice of the test case. Otherwise, a deterministic test case will only be able to test the part of the test purpose that corresponds to the (necessarily fixed) way the test case resolves the choice. On the other hand, a choice that can be resolved simultaneously by the test case and SUT leads to problems because it might lead to a race condition where both test case and SUT resolve the choice in an inconsistent manner. This situation bears strong resemblance to the presence of non-local choice in the MSC [1].

Figure 5 shows examples of malformed MSCs: in m_5 exist $\mathbf{x}, \mathbf{y} \in X_{m_5} \upharpoonright \Sigma_o$ with $\mathbf{x} \neq \mathbf{y}$ and $\sigma = !_{r,p}a \cdot ?_{p,r}b \in \text{lin}(\mathbf{x}) \cap \text{lin}(\mathbf{y}) \neq \emptyset$, and hence WF_1 is violated. Indeed there exist \mathbf{x}, \mathbf{y} with that property such that $v_{m_5}(\mathbf{x}) = \text{pass}$ and $v_{m_5}(\mathbf{y}) = \text{fail}$. Taking into account the fact that a test system will only observe σ it is clear that m_5 does not describe testable behaviour—which verdict should a test system assign after observing σ ? The MSC m_6 is malformed because it violates WF_2 : ε is a choice point for the actions $!_{r,p}a_1$, $!_{r,p}a_2$, and $!_{p,r}c$. In its initial configuration, the test system can either (deterministically) send a_1 or a_2 , but will then not be able to test the behaviour of the SUT that corresponds to the respective other choice. Also, what happens if the test system decides to perform action $!_{r,p}a_1$ while the SUT, before it has received a_1 , performs $!_{p,r}c$? This behaviour is not defined by the MSC. For an example of a well-formed MSC, the reader may verify that m_3 from Fig. 2 is indeed well-formed.

3 Test Case Validity

We now define the validity of a test case w. r. t. a well-formed test purpose. Our definition is different from the available conformance relations for labeled transition systems because it assigns different roles to test case and SUT. We show that the well-formedness conditions on MSCs from the previous section suffice to guarantee the existence of a valid test case. Moreover, we give a simple decision procedure that decides validity of a test case and prove its correctness.

First, we need to formalize the notion of a test case. Intuitively, a test case interacts with the SUT by means of exchanging messages and finally assigning a verdict. Formally, we model a test case as follows:

Test Cases. A test case is a partial function $\mathcal{T} : \Sigma_o^* \rightarrow \Sigma_o^! \dot{\cup} \{\delta\} \dot{\cup} V_f$, where δ is a symbol that denotes *quiescence* of the test case.

A run of a test case \mathcal{T} is a sequence $\sigma_0, \sigma_1, \dots, \sigma_n$, of words from Σ_o^* such that $\sigma_0 = \varepsilon$, and $\sigma_i \xrightarrow[\mathcal{T}]{} \sigma_{i+1}$ for $0 \leq i < n$, where the relation $\xrightarrow[\mathcal{T}]{} is defined by$

$$\sigma \xrightarrow[\mathcal{T}]{} \sigma a \Leftrightarrow_{\text{df}} \mathcal{T}(\sigma) \text{ defined \& } (\mathcal{T}(\sigma) = a \in \Sigma_o^! \vee \mathcal{T}(\sigma) = \delta \& a \in \Sigma_o^?)$$

A run $\sigma_0, \sigma_1, \dots, \sigma_n$ is called *complete* if $\mathcal{T}(\sigma_n) \in V_f$. Note that it is indeed impossible to extend a complete run due to the definition of $\xrightarrow[\mathcal{T}]{}.$

In the following we will show how to model test case validity as a certain language inclusion problem.

Test Languages. Both the runs of a test case and the tester observable traces of a well-formed test purpose naturally induce *test languages*, i. e., languages $L \subseteq \Sigma_o^*$ together with a verdict assignments v_L :

For a test case \mathcal{T} , the test language $\langle L_{\mathcal{T}}, v_{\mathcal{T}} \rangle$ is defined by $L_{\mathcal{T}} =_{\text{df}} \{\sigma \in \Sigma_o^* : \varepsilon \xrightarrow[\mathcal{T}]{}^* \sigma\}$ with verdict assignment $v_{\mathcal{T}}$ defined by

$$v_{\mathcal{T}}(\sigma) =_{\text{df}} \begin{cases} \mathcal{T}(\sigma), & \text{if } \mathcal{T}(\sigma) \in V_f; \\ \text{none}, & \text{otherwise.} \end{cases}$$

For a well-formed test purpose \mathcal{M} , the induced test language $\langle L_{\mathcal{M}}, v_{\mathcal{M}} \rangle$ is defined by setting $L_{\mathcal{M}} =_{\text{df}} \text{obs}(X_{\mathcal{M}})$ and, for $\sigma \in L_{\mathcal{M}}$, $v_{\mathcal{M}}(\sigma) =_{\text{df}} v_{\mathcal{M}}(\mathbf{x})$ for the (due to WF_1 uniquely defined) $\mathbf{x} \in X_{\mathcal{M}}$ with $\sigma \in \text{obs}(\mathbf{x})$.

It can easily be shown that $v_{\mathcal{T}}$ and $v_{\mathcal{M}}$ are well-defined and satisfy the requirements imposed on verdict assignments.

What is the correct relation between $\langle L_{\mathcal{M}}, v_{\mathcal{M}} \rangle$ and $\langle L_{\mathcal{T}}, v_{\mathcal{T}} \rangle$ to define validity of \mathcal{T} w. r. t. \mathcal{M} ? Clearly, $v_{\mathcal{M}}$ and $v_{\mathcal{T}}$ should agree on $L_{\mathcal{M}} \cap L_{\mathcal{T}}$. But what is the right relations between $L_{\mathcal{M}}$ and $L_{\mathcal{T}}$? None of the “obvious” choices leads to a satisfactory notion of validity:

- if we would require $L_{\mathcal{M}} \subseteq L_{\mathcal{T}}$ then there would be no valid test cases for any test purpose that allows (inessential) choice between two actions $a, b \in \Sigma_o^!$ because $L_{\mathcal{M}}$ contains traces for both choices while a deterministic test case would be limited to only a single choice.

```

valid(test_purpose  $\mathcal{M}$ ; test_case  $\mathcal{T}$ ; string  $\rho$ ) {
  if  $\mathcal{T}(\rho)$  is undefined then fail;
  if  $\mathcal{T}(\rho) \in V_f$  &  $\mathcal{T}(\rho) \neq v_{\mathcal{M}}(\rho)$  then fail;
  else if  $\mathcal{T}(\rho) = \delta$  then
    if  $en(\mathcal{M}, \rho) \cap \Sigma_o^? = \emptyset$  then fail;
    else foreach  $a \in en(\mathcal{M}, \rho) \cap \Sigma_o^?$  do  $valid(\mathcal{M}, \mathcal{T}, \rho \cdot a)$ ;
  else if  $\rho \cdot \mathcal{T}(\rho) \notin L_{\mathcal{M}}$  then fail;
  else  $valid(\mathcal{M}, \mathcal{T}, \rho \cdot \mathcal{T}(\rho))$ ;
  success;
}

```

where $en(\mathcal{M}, \rho) =_{df} \{a \in \Sigma_o : \rho \cdot a \in obs(X_{\mathcal{M}})\}$

Algorithm 1. Validation algorithm.

- requiring $L_{\mathcal{T}} \subseteq L_{\mathcal{M}}$ would allow the test case to send arbitrary messages to the SUT even though these would not be specified in the test purpose
- if we require $L_{\mathcal{T}} \cap L_{\mathcal{M}} \neq \emptyset$ then the test case would only be required to react to one of the possible many (essential) choices that the SUT might have.

While the first option matches the intuitive meaning of test case validity best, it needs to be modified to eliminate the influence of inessential choice. This is done by means of the following equivalence relation on strings:

Let $L \subseteq \Sigma_o^*$ be a language. We define an equivalence relation $\simeq_L \subseteq L \times L$ by setting $\sigma \simeq_L \rho \Leftrightarrow_{df} \rho$ is a permutation of σ such that $\sigma \upharpoonright \Sigma_o^? = \rho \upharpoonright \Sigma_o^?$. The *equivalence class* w. r. t. \simeq_L of $\sigma \in L$ is denoted by $[\sigma]_L =_{df} \{\rho \in L : \sigma \simeq_L \rho\}$.

Test Case Validity. Let \mathcal{M} be a well-formed test purpose and \mathcal{T} be a test case for \mathcal{M} . Then \mathcal{T} is called a *valid* test case w. r. t. \mathcal{M} if

- for every $\sigma \in L_{\mathcal{T}} \cap L_{\mathcal{M}}$, $v_{\mathcal{T}}(\sigma) = v_{\mathcal{M}}(\sigma)$, and
- for every $\sigma \in L_{\mathcal{M}}$ with $v_{\mathcal{M}}(\sigma) \in V_f$, $[\sigma]_{L_{\mathcal{M}}} \cap L_{\mathcal{T}} \neq \emptyset$.

Since we have given the definition both for well-formed test purposes and test case validity, it would be futile to use one to justify the other. What can be shown formally though, is that these notions are compatible in the following sense:

Theorem 1. *Let \mathcal{M} be a well-formed test purpose. Then there exists a test case \mathcal{T} that is valid w. r. t. \mathcal{M} . \mathcal{T} can be computed effectively from \mathcal{M} .*

Also, it is easy to see that there are MSCs that violate one of the well-formedness conditions, for which no valid test case exists.

Deciding Validity. In the following we present an algorithm that decides validity of a test case w. r. t. a well-formed test purpose and establish the algorithm's correctness. Interestingly, the algorithm does not require the calculation of the $\simeq_{L_{\mathcal{M}}}$ -classes but only refers to $obs(X_{\mathcal{M}})$, $v_{\mathcal{M}}$, and $L_{\mathcal{M}}$, which can easily be derived from \mathcal{M} .

Theorem 2. *Let \mathcal{M} a well-formed test purpose and \mathcal{T} a test case for \mathcal{M} . Then \mathcal{T} is valid w. r. t. \mathcal{M} iff $valid(\mathcal{M}, \mathcal{T}, \varepsilon)$ does not fail.*

4 Practical Considerations

The previous sections have discussed formally the relationship between a test purpose defined using MSC and a test system that implements the test purpose. No assumptions have been made on the test system besides that it is deterministic and that it has observable test events and a final verdict status. An MSC based validator tool has been designed and developed within a joint project between Nokia Research Center and Fraunhofer FOKUS.

The validator is designed to run against any test system that provides some basic functionality, like starting of a test case, retrieving the status of the final verdict, sending and receiving messages, etc. The basic idea was to create a validator that is not only able to validate the abstract test suite but also a real test system (tester), i. e., an abstract test suite plus its execution environment plus the glue that is necessary to tie the test suite to the actual system under test. Since this glue can be of considerable complexity, e.g., consisting of implementations of various protocol stacks, message en- and decoders, possibly tailored hardware, etc., testing of the whole test system is indeed an important aspect.

This is also one of the advantages of our approach as compared to other approaches like an isolated verification of the abstract test suite or an automatic generation of test cases from test purposes.

Given a sufficiently detailed specification of the test purpose, a combination of automatic generation of test cases [14] from the test purpose together with a validation following our approach seems optimal. The validation guarantees both the correctness of the implementation of the generation algorithm and of the additional components that make up the test system.

The design of the validator aims to make it as independent of the test system as possible by defining a small, well-defined interface to connect the validator to the test system. In our case study we have used a TTCN-3 test system with the MSC validator. The validator accesses the test system at its (proprietary) control interface to trigger the execution of testcases and retrieve the final verdict. It uses TTCN-3's standardized communication interface toward the SUT [13] to exchange messages with the test system. The MSC validator has been implemented using JAVA and the test system runs independently of the validator. Although not all work within this project has been completely finished, results so far show that using MSCs as test purpose definition language and as basis for the test case validation can improve the quality of test cases and thus the quality of system implementations.

Future Work

This paper defines a novel approach to test case validation and provides the necessary theoretical background. Yet, it is only a first step toward a working test case validation system. In particular, the following issues need to be addressed in the future:

Algorithms and Complexity. Deciding well-formedness of an MSC \mathcal{M} so far requires the calculation of the semantics $X_{\mathcal{M}}$, which is a costly operation. A syntactic characterization of well-formedness would be desirable because it would probably allow for faster tests for well-formedness that could, e.g., also be built into an MSC editor to support test

purpose development by pointing out problematic constructs. Additionally, a detailed analysis of the complexity of well-formedness and test case validity would be desirable.

Data. Since its last revision, data is an integral part of the MSC language. An extension of our approach that also takes into account data passed in messages is essential for the practical applicability of our approach to a wider class of test cases. While this should not impose any theoretical problems, it will be a challenge to integrate data into the implementation in a user-friendly manner.

Time. MSCs allow to express various timing constraints and timing aspects are important in many testing efforts. Therefore, we plan to extend our approach to MSCs with timing constraints. From a theoretical point of view, this is probably the most interesting way to continue the work presented in this paper.

5 Appendix

This appendix contains the proofs of Theorems 1 and 2 (for technical reason in reverse order). In the following, let \mathcal{M} denote a well-formed test purpose.

From property WF_1 we get that the function $\langle \cdot \rangle_{\mathcal{M}} : \text{obs}(X_{\mathcal{M}}) \rightarrow X_{\mathcal{M}}$ that maps every $\sigma \in \text{obs}(X_{\mathcal{M}})$ to a $\mathbf{x}_{\sigma} \in X_{\mathcal{M}}$ such that $\sigma \in \text{lin}(\mathbf{x}_{\sigma})$ is in fact a well-defined and total. It is easy to show the following property:

Lemma 3. *Let \mathcal{M} be a well-formed test purpose and $\rho, \sigma \in \text{obs}(X_{\mathcal{M}})$ with $\rho \leq \sigma$. Then $\langle \rho \rangle_{\mathcal{M}} \leq \langle \sigma \rangle_{\mathcal{M}}$.*

Let \mathcal{M} be a well-formed test purpose, \mathcal{T} a test case for \mathcal{M} and $\sigma \in L_{\mathcal{M}}$ with $v_{\mathcal{M}}(\sigma) \neq \text{none}$. A *validation* for σ is a complete run $\rho_0 \xrightarrow{\mathcal{T}} \rho_1 \xrightarrow{\mathcal{T}} \dots \xrightarrow{\mathcal{T}} \rho_n$ such that $\rho_n \simeq_{L_{\mathcal{M}}} \sigma$ and $v_{\mathcal{T}}(\rho_n) = v_{\mathcal{M}}(\sigma)$.

It is easy to see that validity of a test case w. r. t. a test purpose can equivalently be formulated as follows.

Lemma 4. *Let \mathcal{M} be a well-formed test purpose and \mathcal{T} a test case for \mathcal{M} . Then \mathcal{T} is valid w. r. t. \mathcal{M} iff every $\sigma \in L_{\mathcal{M}}$ has a validation.*

We will need the following technical lemma:

Lemma 5. *Let \mathcal{M} be a well-formed test purpose, $a, b \in \Sigma_o$ be actions, and $\rho, \sigma \in \Sigma_o^*$. Moreover, assume $\rho a, \rho b \in L_{\mathcal{M}}$, $v_{\mathcal{M}}(\sigma) \neq \text{none}$, and $\rho b \leq \sigma$. If $a \notin \Sigma_o^!$ or $b \notin \Sigma_o^!$ (or both), then there exists a $\sigma' \in L_{\mathcal{M}}$ with $\sigma \simeq_{L_{\mathcal{M}}} \sigma'$, $v_{\mathcal{M}}(\sigma) = v_{\mathcal{M}}(\sigma')$, $\rho a \leq \sigma'$, and $v_{\mathcal{M}}(\sigma) = v_{\mathcal{M}}(\sigma')$.*

Proof. Let a, b, ρ, σ as required by the lemma and let $\mathbf{x} = \langle \rho \rangle_{\mathcal{M}}$, and $\mathbf{z} = \langle \sigma \rangle_{\mathcal{M}}$. Let $\mathbf{y}_a, \mathbf{y}_b \in X_{\mathcal{M}} \upharpoonright \Sigma_o$ such that $\mathbf{y}_a = \mathbf{x} \circ_c a$ and $\mathbf{y}_b = \mathbf{x} \circ_c b$. From WF_1 we get $\mathbf{x} \leq \mathbf{y}_b \leq \mathbf{z}$. From WF_2 , also $\mathbf{x} \leq \mathbf{y}_a \leq \mathbf{z}$ holds. Hence, there exists $\mathbf{u} \in X_{\mathcal{M}} \upharpoonright \Sigma_o$ with $\mathbf{u} = \mathbf{x} \circ_c a \circ_c b$ and $\mathbf{u} \leq \mathbf{z}$ and we obtain σ' setting $\sigma' = \rho a b \eta$, where η is the string that can be appended to ρb to obtain σ with the first occurrence of a deleted. From what have said before, σ' is a linearization of \mathbf{z} , hence $\sigma \simeq_{L_{\mathcal{M}}} \sigma'$ and $v_{\mathcal{M}}(\sigma) = v_{\mathcal{M}}(\sigma')$.

Proof (Proof of Theorem 2). Assume that $\mathbf{valid}(\mathcal{M}, \mathcal{T}, \varepsilon)$ does not fail and let $\sigma \in L_{\mathcal{M}}$ with $v_{\mathcal{M}}(\sigma) \neq \text{none}$ and $|\sigma| = n$. By Lemma 4, it suffices to show that there exists a validation of σ . To this purpose, we will construct sequences ρ_0, \dots, ρ_n and $\sigma_0, \dots, \sigma_n$ such that $|\rho_i| = i$, $\mathbf{valid}(\mathcal{M}, \mathcal{T}, \rho_i)$ is called during the execution of the algorithm, $\rho_i \leq \sigma_i$, $\sigma_i \simeq_{L_{\mathcal{M}}} \sigma$, and $v_{\mathcal{M}}(\sigma) = v_{\mathcal{M}}(\sigma_i)$, for each $0 \leq i \leq n$.

We start with $\rho_0 = \varepsilon$ and $\sigma_i = \sigma$, which satisfies all the required properties. Assume that the sequences have been constructed up to i . Since $\mathbf{valid}(\mathcal{M}, \mathcal{T}, \rho_i)$ does not fail, $\rho_i \in L_{\mathcal{M}}$ holds and there are the following possibilities:

- $\mathcal{T}(\rho) \in V_{\mathcal{F}}$ & $\mathcal{T}(\rho) = v_{\mathcal{M}}(\rho)$. In this case, $|\rho| = n$ must hold because otherwise $v_{\mathcal{M}}(\sigma_i) \neq \text{none}$ and $v_{\mathcal{M}}(\rho_i) \neq \text{none}$, together with $\rho_i < \sigma_i$, would be (by Lemma 3) a contradiction to the fact that $v_{\mathcal{M}}$ is a verdict assignment on $L_{\mathcal{M}}$.
- $\mathcal{T}(\rho) = \delta$ & $\mathbf{en}(\mathcal{M}, \rho) \cap \Sigma_o^? \neq \emptyset$. Then $i < n$ must hold and since $\rho_i < \sigma_i$, there exists $b \in E_c(T)$ such that $\rho_i b \leq \sigma_i$. If $b \in \Sigma_o^?$ then there will be a call $\mathbf{valid}(\mathcal{M}, \mathcal{T}, \rho_i b)$ and we set $\rho_{i+1} =_{\text{df}} \rho_i b$ and $\sigma_{i+1} =_{\text{df}} \sigma_i$ to continue the sequences. Clearly, this satisfies all necessary properties. If $b \in \Sigma_o^!$ then let $a \in \mathbf{en}(\mathcal{M}, \rho_i) \cap \Sigma_o^?$. Then a, b, ρ_i, σ_i satisfy the prerequisites of Lemma 5, which yields the existence of $\sigma'_i \in L_{\mathcal{M}}$ with $\sigma_i \simeq_{L_{\mathcal{M}}} \sigma'_i$, $v_{\mathcal{M}}(\sigma_i) = v_{\mathcal{M}}(\sigma'_i)$, and $\rho_i a \leq \sigma'_i$. If we set $\rho_{i+1} =_{\text{df}} \rho_i a$ then we have extended the sequence as required.
- $\mathcal{T}(\rho) = a \in \Sigma_o^!$ & $\rho a \in L_{\mathcal{M}}$. In this case we necessarily have to set $\rho_{i+1} =_{\text{df}} \rho_i a$ and we need to show the existence of a suitable σ_{i+1} . This can be done similar to the previous case using Lemma 5.

It is easy to see that $\mathcal{T}(\rho_n) \in V_{\mathcal{F}}$ and by construction it holds that $\rho_n \simeq_{L_{\mathcal{M}}} \sigma$ as well as $v_{\mathcal{T}}(\rho_n) = v_{\mathcal{M}}(\sigma)$. Moreover, obviously $\rho_0 \xrightarrow{\mathcal{T}} \dots \xrightarrow{\mathcal{T}} \rho_n$ is complete run and thus we have found the desired validation for σ .

For the converse direction, let \mathcal{T} be a test case that is valid w. r. t. \mathcal{M} . We need to show that the call $\mathbf{valid}(\mathcal{M}, \mathcal{T}, \varepsilon)$ does not fail. Hence assume that it does fail and let $\rho \in L_{\mathcal{M}}$ a prefix-maximal word such that $\mathbf{valid}(\mathcal{M}, \mathcal{T}, \rho)$ is evaluated. By definition of \mathbf{valid} , $\rho \text{ in } L_{\mathcal{M}}$ must hold. One of the following choices for ρ is the one that leads to failure.

- $\mathcal{T}(\rho)$ is undefined, then obviously, for every $\sigma \in L_{\mathcal{M}}$ with $\rho \leq \sigma$, $[\sigma]_{L_{\mathcal{M}}} \cap L_{\mathcal{T}} = \emptyset$.
- $\mathcal{T}(\rho) \in V_{\mathcal{F}}$ and $\mathcal{T}(\rho) \neq v_{\mathcal{M}}(\rho)$, which violates the first condition in the definition of test case validity.
- $\mathcal{T}(\rho) = \delta$ and $\mathbf{en}(\mathcal{M}, \rho) \cap \Sigma_o^? = \emptyset$. If $v_{\mathcal{M}}(\rho) \neq \text{none}$ then $L_{\mathcal{T}}$ and $L_{\mathcal{M}}$, then again the first condition of the definition of test case validity is violated. If $v_{\mathcal{M}}(\rho) = \text{none}$ then there exists $\sigma \in L_{\mathcal{M}}$ with $v_{\mathcal{M}}(\sigma) \neq \text{none}$ and $\rho < \sigma$. It is easy to see that, if there exists $\eta \in [\sigma]_{L_{\mathcal{M}}} \cap L_{\mathcal{T}}$, then $\rho < \eta$, but since $\mathcal{T}(\rho) = \delta$ and $\mathbf{en}(\mathcal{M}, \rho) \cap \Sigma_o^? = \emptyset$, for every $\chi \in L_{\mathcal{T}}$ with $\rho < \chi$, $\chi \notin L_{\mathcal{M}}$ holds and hence there does not exist such a η .
- The case that $\mathcal{T}(\rho) = a \in \Sigma_o^!$ but $\rho \cdot a \notin L_{\mathcal{M}}$ is analog to the previous case.

Hence, $\mathbf{valid}(\mathcal{M}, \mathcal{T}, \varepsilon)$ cannot fail.

Proof (Proof of Theorem 1). We define a test case \mathcal{T} as follows: for $\sigma \in \text{obs}(X_{\mathcal{M}})$:

$$\mathcal{T}(\sigma) =_{\text{df}} \begin{cases} v_{\mathcal{M}}(\langle \mathbf{x} \rangle_{\mathcal{M}}), & \text{if } \mathbf{en}(\mathcal{M}, \sigma) = \emptyset; \\ \delta, & \text{if } \emptyset \neq \mathbf{en}(\mathcal{M}, \sigma) \subseteq \Sigma_o^? \\ a, & \text{for an arbitrary } a \in \mathbf{en}(\mathcal{M}, \sigma) \cap \Sigma_o^! \text{ otherwise} \end{cases}$$

It is easy to see that for this test case \mathcal{T} , $\mathbf{valid}(\mathcal{M}, \mathcal{T}, \varepsilon)$ does indeed not fail and hence, by Theorem 2, \mathcal{T} is a valid test case w. r. t. \mathcal{M} .

References

1. H. Ben-Abdallah and S. Leue. Syntactic detection of process divergence and non-local choice in message sequence charts. In E. Brinksma, editor, *Tools and Algorithms for the Construction and Analysis of Systems*, volume 1217 of *Lecture Notes in Computer Science*, pages 259–274. Springer Verlag, 1997.
2. P. Deussen. Concurrent automata. Technical Report 1-05/1998, Brandenburg Tech. Univ. Cottbus, 1998.
3. ETSI. The tree and tabular combined notation version 3; part 1: TTCN-3 core language. Technical Report ES 201 873-1, ETSI, 2001.
4. J. Grabowski. On partial languages. *Fundamenta Informaticae*, 4(2):427–498, 1981.
5. J. Grabowski and D. Hogrefe. TTCN SDL- and MSC-based specification and automated test case generation for inap. In *Proceedings of the 8th International Conference on Telecommunication Systems (ICTS'2000) - Modeling and Analysis*, Nashville, March 2000.
6. ITU-T. ITU-T recommendation z.120 message sequence chart (MSC). Technical report, ITU-T, 1999.
7. B. Jonsson and G. Padilla. An execution semantics of MSC-2000. In R. Reed and J. Reed, editors, *Proceedings of the 10th International SDL-Forum*, number 2078 in *Lecture Notes in Computer Science*. Springer Verlag, 2001.
8. J.-P. Katoen and L. Lambert. Pomsets for message sequence charts. In *Proc. of 1st Workshop of the SDL Forum Society on SDL and MSC, SAM98*, Berlin, 1998.
9. S. Mauw and M. A. Reniers. Operational semantics for MSC'96. In A. Cavalli and D. Vincent, editors, *Tutorials of the Eighth SDL Forum SDI'97: Time for Testing - SDL, MSC and Trends*, pages 135–152, Evry, France, 1997. Institut national des télécommunications.
10. A. Mazurkiewicz. Introduction to trace theory. In V. Diekert and G. Rozenberg, editors, *The Book of Traces*, chapter 1, pages 3 – 42. World Scientific, Singapore – New Jersey – London – Hong Kong, 1995.
11. V. Pratt. Modelling concurrency with partial orders. *International Journal of Parallel Programming*, 15(1):33–71, 1986.
12. R. Scheurer, J. Grabowski, and D. Hogrefe. Revised comparison of an automatically generated and a manually specified test suite for the B-ISDN protocol SSCOP. In H. König and P. Langendörfer, editors, *FBT'98 - Formale Beschreibungstechniken für verteilte Systeme*. Shaker Verlag, Aachen, 1998. Available online from <http://www.itm.mu-luebeck.de/>.
13. S. Schulz and T. Vassiliou-Gioles. Implementation of TTCN-3 test systems using the TRI. In I. Schieferdecker, K. H. and A. Wolisz, editors, *Testing of Communication Systems XIV, Proc. of TestCom-2002*, pages 425–442, Berlin, Germany, 2002. Kluwer Academic Publishers.
14. M. Schmitt, M. Ebner, and J. Grabowski. Test generation with autolink and testcomposer. In *Proceedings of the 2nd Workshop of the SDL Forum Society on SDL and MSC (SAM'2000)*. SDL Forum Society, 2000. Proceedings available online from <http://www.irisa.fr/manifestations/2000/sam2000/>.