Test selection for traces refinement
Ana Cavalcanti, Marie-Claude Gaudel

To cite this version:

HAL Id: hal-01126800
https://hal.archives-ouvertes.fr/hal-01126800
Submitted on 6 Mar 2015
Test selection for traces refinement

Ana Cavalcanti
University of York, Department of Computer Science
York YO10 5GH, UK

Marie-Claude Gaudel
LRI, Université de Paris-Sud and CNRS
Orsay 91405, France

Abstract

Theories for model-based testing identify exhaustive test sets: typically infinite sets of tests whose execution establishes the conformance relation of interest. Practical techniques rely on selection strategies to identify finite subsets of these tests, and popular approaches are based on requirements to cover the model. In previous work, we have defined testing theories for refinement-based process algebra, namely, CSP and Circus, a state-rich process algebra. In this paper, we consider the selection of tests designed to establish traces refinement. In this case, conformance does not require that all traces of the model are available in the system under test, and this can raise challenges regarding coverage criteria for selection. To address these difficulties, we present a framework for formalising a variety of selection strategies. We exemplify its use in the formalisation of a selection criterion based on coverage of process communications for integration testing. We consider models written in Circus, whose symbolic testing theory facilitates the definition of uniformity and regularity hypotheses based on data operations, but also imposes extra challenges for selection of concrete tests. Our results, however, are relevant for any formalism where the conformance relation does not require all the traces of the specification to be executable by the system under test.

Keywords: process algebra, CSP, Circus, synchronisation coverage, integration testing

1. Introduction

We address in this paper the issue of selecting tests when using an abstract specification for testing that a system behaves like one of its refinements. In particular, we are interested in models written using process algebra like CSP [51] or Circus [17], and in traces refinement in that context.

CSP is a well established notation that has been in use for more than twenty years. The availability of a powerful model checker has led to acceptance both in academia and industry. In the public domain, we have reports on applications in hardware and e-commerce [2, 26], for example. CSP has been combined with a number of data-modelling languages to define notations that cope with state-rich reactive systems [21, 36, 52, 49]; Circus is one of these combinations with Z [62]. Circus has been used for modelling and verification of control systems specified in Simulink [9, 38]. It is currently being used to verify aerospace applications, including virtualisation software by the US Naval Research Laboratory [23].

The traditional area of application for CSP and Circus is refinement-based development and verification, not testing, but whenever a CSP or a Circus model is available, the possibility of using it for testing is attractive, especially in industry. Moreover, when the correctness criterion for development is refinement, it is natural to adopt that same criterion for testing. We have previously developed testing theories for CSP [10] and Circus [13]. We base our discussions here on the theory for Circus, which extends and generalises that for CSP. In addition, it enables richer selection strategies based on data types (as well as traces).
The various notions of refinement adopted in the context of CSP and Circus require that the set of traces of an implementation is included in that of the specification; in particular, this is exactly the definition of traces refinement. Selection of tests for traces refinement is challenging because it is acceptable that some traces of the specification are not implemented by the system under test (SUT). It may, therefore, be the case that some selected tests are not executable. As a consequence, given a selection criterion, the selection cannot be performed statically only. At runtime, the test driver must ensure that alternative tests are submitted until the criterion is fulfilled, or until it is certain that it cannot, due to lack of traces necessary to its fulfillment. In other words, any testing strategy requires a combination of some selection criterion with a driver designed to ensure that the selection criterion will be reached at run time, if it is possible.

Our main contributions are as follows. First, we propose a formal framework for selection based on the definition of an exhaustive set of tests that can contribute to the fulfillment of the selection criterion and of a test driver. Additionally, we consider symbolic tests, which pose a challenge of the same nature for obtaining concrete tests that can be used by the driver, since it is acceptable that some or all instantiations are not implemented. Symbolic tests lead to a two-level selection method, where first some symbolic tests are selected, and then we select some of their instantiations, which are submitted until the criterion is fulfilled. Finally, as an application of our new framework, we consider coverage of communications between parallel processes of a Circus model; we present a complete formalisation of this selection criterion.

Our work bears some similarity with the dynamic test generation techniques [6], where symbolic execution is used at runtime to ensure coverage of all feasible paths of a program text. Here, however, the issue is not infeasibility, but arbitrary partial implementation of traces. Moreover, we are concerned with selection criteria that are based on requirements to exercise elements of the model, not the SUT. Our framework also has some similarities with adaptive testing [33], which is aimed at tackling nondeterminism in implementations rather than partial implementation of traces. In contrast, for coverage of behaviours of a nondeterministic SUT, we rely on the complete testing assumption [24], which may, in special cases, be enforced by techniques similar to those used in reachability testing [34, 39].

In the next section, we give an overview of Circus and its testing theory. Section 3 presents our novel framework for selection. In Section 4, we formalise a synchronisation coverage criterion for use with our framework, and we define finite test sets and suitable drivers. We consider related works in Section 5, and conclude in Section 6 with a discussion of our results and future work.

2. Circus and its testing theory

In this section, we cover the background material for our work: we describe Circus using an example of a simple protocol, and introduce the main concepts of its testing theory.

2.1. An overview of Circus

In Figure 1, we present a Circus model for a simple protocol for communication between a Sender and a Receiver via a Medium that can corrupt at most one out of three messages. Systems and their components are modelled in Circus using processes. These encapsulate some state and interact with each other and their environment via channel communications, which are synchronous, atomic, and instantaneous events. In Figure 1, we have a model that uses four channels, in, out, left, and right, and introduces five processes: Medium, Sender, Receiver, Components, and Protocol.

We observe that, although Circus events (channel communications) are synchronous, this example shows that its modelling paradigm is rich enough to cater for asynchronous systems. Our example models an asynchronous communication between the Sender and the Receiver by identifying the relevant interaction points of the asynchronous transaction (using the channels left and right).

A Circus model is formed by a sequence of paragraphs. In Figure 1, the first paragraph defines a set Bit including 0 and 1. The messages exchanged using the specified protocol are bits. In the second paragraph, we declare the channels, whose type Bit defines that they are used to communicate bits.

The next three paragraphs in Figure 1 introduce (basic) processes by (explicitly) defining their states and behaviour. Process states are defined using Z schemas. The state of the process Medium has a single
of
A
is assigned to
through the channel
left
causes of a medium error, so that the occurrence of an error becomes completely arbitrary.

right
the channel
left
that a corrupt message is sent. In this case, we have a nondeterministic choice between outputting through
communication
behaviour in which, after the communication
c which introduces the local name
X
through the channel
left
that a corrupt message can be sent immediately. Afterwards, a recursive action iteratively accepts messages
if the value of
noE
terminates immediately without changing the state. If the other action is chosen, after the output, the value
of
noE
is updated to indicate that the next two communications must not be corrupt. In the conditional,
if the value of
noE
is not 0, then
right!x
takes place, and the value of
noE
is decremented.

The process
Sender
has no state. Its action defines that it accepts an input
m
through the channel
in
and sends it three times to the
Medium
through the channel
left
, before recursing and starting again.

The
Receiver
process, on the other hand, keeps a bag of bits
ms
in the state. At each iteration of the

component
noE
recording the number of messages that must be sent correctly before another error is possible. We use this information to model the assumption that at most one out of every three messages is corrupted. The declaration of
noE
indicates that it can only take the values 0, 1, and 2.

After the
•
, we have a
Circus
action that specifies the behaviour of
Medium
. It is written using a combination of CSP operators and guarded commands. First of all, an assignment initialises
noE
to 0, so that a corrupt message can be sent immediately. Afterwards, a recursive action iteratively accepts messages through the channel
left
and sends them through
right
. Recursion is defined using the operator
µX • A(X)
, which introduces the local name
X
for the action
A
, in which references to
X
are recursive calls.

In the body of the recursion in
Medium
, we have an input communication
left?x
that accepts an input through the channel
left
and records it in the local variable
x
. The prefixing operator
m → A
describes a behaviour in which, after the communication
m
, we have the execution of the action
A
. In
Medium
, after the communication
left?x
, we have a conditional that checks the value of
noE
. If it is 0, then it is possible that a corrupt message is sent. In this case, we have a nondeterministic choice between outputting through the channel
right
the input
x
(comunication
right!x
) or the corrupt value
1 − x
, in which case the value
2
is assigned to
noE
. The nondeterministic choice operator
A_1 \cap A_2
chooses arbitrarily between the execution of
A_1
or
A_2
. In our example, the nondeterminism reflects the fact that we are abstracting from the possible causes of a medium error, so that the occurrence of an error becomes completely arbitrary.

If the action chosen is
right!x → Skip
, then after the output over
right
, it behaves like
Skip
, which terminates immediately without changing the state. If the other action is chosen, after the output, the value of
noE
is updated to indicate that the next two communications must not be corrupt. In the conditional,
if the value of
noE
is not 0, then
right!x
takes place, and the value of
noE
is decremented.

The process
Sender
has no state. Its action defines that it accepts an input
m
through the channel
in
and sends it three times to the
Medium
through the channel
left
, before recursing and starting again.

The
Receiver
process, on the other hand, keeps a bag of bits
ms
in the state. At each iteration of the

Figure 1: Circus example: a simple protocol

\( \text{Bit} \equiv \{0, 1\} \)

\[
\text{process Medium} \equiv \begin{align*}
\text{state MS} & \equiv [\text{noE} : 0 \ldots 2] \\
\bullet \text{noE} & \equiv 0 ; \left( \mu X \bullet \left( \left( \begin{align*}
& \text{left?}x \rightarrow \begin{cases}
& \text{if } \text{noE} = 0 \rightarrow \text{Skip} \cap \text{right!(1 − }x\text{) → noE := 2) if } \\
& \text{noE} > 0 \rightarrow \text{right!}x \rightarrow \text{noE} := \text{noE} − 1 \\
& \end{cases}
\end{align*} \right) \right) ; X \right) 
\end{align*}
\]

\[
\text{process Receiver} \equiv \begin{align*}
\bullet (\mu X \bullet \text{in?}m \rightarrow \text{left!}m \rightarrow \text{left!}m \rightarrow \text{left!}m \rightarrow X) 
\end{align*}
\]

\[
\text{process Components} \equiv \text{Sender} \parallel \text{Receiver} 
\]

\[
\text{process Protocol} \equiv (\text{Components} [\{0 \text{ left, right}\} \text{ Medium}) \setminus \{0 \text{ left, right}\} \]


recursion in its action, the bag is emptied \((ms := []\)) , three messages \(m_1, m_2\), and \(m_3\) are accepted (from the Medium) through right. These messages are stored in \(ms\), and then the bit \((maj ms)\) with the majority of occurrences in \(ms\) is output through out. (The definition of \(maj ms\) is omitted in Figure 1.)

Circus processes can also be combined using CSP operators. In our example, the components connected by the protocol are modelled by the process Components, defined by the interleaving of the processes Sender and Receiver. This reflects the fact that these processes are executed in parallel and independently. The Protocol process itself is defined in terms of the parallel composition of Components and Medium. In this case, we have a parallelism, rather than an interleaving, because these processes need to synchronise on communications over the channels left and right. In a parallelism \(P_1 \parallel cs P_2\), the processes \(P_1\) and \(P_2\) proceed independently, except only for communications on channels in the given set \(cs\), on which they are required to synchronise. In particular, the state of \(P_1\) is not visible to \(P_2\), and vice-versa.

In the definition of Protocol, we also use hiding. In a process \(P \setminus cs\) the communications over the channels in the set \(cs\) are hidden: they are internal and carried out as soon as possible. In our example, left and right are channels used by the Medium to connect the Components, and so they are internal. Communication with the external environment is realised via the channels in \((\text{used in } \text{Sender})\) and out \((\text{used in } \text{Receiver})\).

We use this and other examples to illustrate our results. Any extra use of Circus notation is explained. The semantics of Circus is defined in a relational style using Hoare and He's Unifying Theories of Programming (UTP) [43]; operational semantics for Circus are defined in [13, 12]. In [12] we define traces refinement using the UTP model. As expected, the definition compares processes \(P_1\) and \(P_2\) with the same alphabet of events, and requires that \(P_1\) is refined by \(P_2\) if, and only if, every trace of \(P_2\) is also a trace of \(P_1\). In the next section, we give an overview of the Circus theory for testing for traces refinement.

2.2. Testing against traces refinement using Circus (and CSP)

In a theory for model-based testing for a particular modelling notation and conformance relation, we identify testability hypotheses, notions of test, test execution, and verdict, and an exhaustive test set. This is a set of tests whose execution and associated verdicts can determine unequivocally whether the SUT behaves in conformance to a given model, as long as the testing hypotheses hold. Typically, this is an infinite set of tests. Here, we consider selection as the definition of a subset of the exhaustive test set. Thus, we briefly recall the definition of the exhaustive test set for Circus and traces refinement [13].

The two testability hypotheses of the Circus theory are standard. First, we assume that the SUT can be described by an (unknown) Circus model. This means, for example, that events are atomic (indivisible) and can be considered as instantaneous: their duration can be neglected when observed at the level of the system. Secondly, we rely on the complete test assumption [24]. It is concerned with possible nondeterminism in the SUT (as opposed to its model); it requires the existence of a number \(n\) such that, if a test is executed \(n\) times, then all possible (nondeterministic) behaviours of the SUT are observed. For a deterministic SUT, \(n\) is 1. When the only source of nondeterminism is due to interleaving of concurrent sequential executions, the complete test assumption can be enforced by the use of reachability-testing techniques to monitor the executions of the SUT. Some of these techniques are briefly presented in Section 5.

The tests of the Circus theory embed the verdict. We use special verdict events inc, pass, and fail used to indicate that a test is inconclusive, because the SUT did not execute the particular trace of events attempted by the test, or that the SUT passed or failed the test. A test is constructed based on a particular trace \(t\) of the model, and a forbidden continuation \(e\) of \(t\). A forbidden continuation is an event that is not allowed after the trace \(t\); in other words, the trace \(t \sqcap (e)\) is not a trace of the model. (We use \((e)\) to denote the singleton sequence containing just the event \(e\), and \(\sqcap\) is the concatenation operator.)

**Example 1.** In our example, \(<in.0, out.0, in.1>\) is a trace of Protocol. The event in.0, for instance, corresponds to a value 0 input through the channel in, and, similarly, out.0, the value 0 output through the channel out. After the trace \(<in.0, out.0, in.1>\), all events out.x, where \(x \neq 1\) are forbidden continuations of Protocol, because after an input of a value 1, just 1 itself can be output.

A test for a trace \(t\) and a forbidden continuation \(e\) attempts to drive the SUT to execute \(t\). If it does not succeed, the test is inconclusive. (As usual, we give an inconclusive verdict when the intended test is
not completed.) If the test does succeed in driving the SUT to execute \( t \), then the forbidden event \( e \) is attempted, and if it is accepted, the SUT fails the test. Otherwise, it succeeds.

**Example 2.** For the trace in Example 1, and forbidden continuation \( \text{out.2} \), we have the test below.

\[
\text{inc} \rightarrow \text{in.0} \rightarrow \text{inc} \rightarrow \text{out.0} \rightarrow \text{inc} \rightarrow \text{in.1} \rightarrow \text{pass} \rightarrow \text{out.2} \rightarrow \text{fail} \rightarrow \text{Stop}
\]

The action \( \text{Stop} \) deadlocks immediately.

The verdict events are interspersed with the events of the trace and the forbidden continuation. The last verdict event before a deadlock determines the verdict of the test. Formally, tests are defined as follows.

**Definition 1.**

\[
T_T(\langle \rangle, e) = \text{pass} \rightarrow e \rightarrow \text{fail} \rightarrow \text{Stop}
\]

\[
T_T(\langle e_1 \rangle \bowtie t, e_2) = \text{inc} \rightarrow e_1 \rightarrow T_T(t, e_2)
\]

In \( T_T(t, e) \), extending the trace \( t \) with \( e \) is supposed to lead to an invalid trace, since \( e \) is supposed to be a forbidden continuation: not an initial after \( t \); as already explained, the test aims at ruling it out.

Execution \( \text{Execution}_{\text{SUT}}^{SP}(T) \) of one of these tests \( T \) is carried out by executing \( T \) and the SUT in parallel, synchronising on all model events (that is, the non-verdict events used in the model and in the SUT). Relying on our first testability hypothesis, we use \( \text{SUT} \) to denote the unknown model of the SUT. We also use \( \Sigma \) to denote the set of model events as defined in the specification \( SP \).

**Definition 2.**

\[
\text{Execution}_{\text{SUT}}^{SP}(T) = (\text{SUT}[\Sigma]T) \setminus \Sigma \text{ where } \Sigma = \alpha SP
\]

The model events are hidden, that is, internal to the experimentation process. This ensures that they are not affected by the environment of the experiment, since they are not visible in the environment. Hiding also ensures that these model events occur as soon as they become available (in the SUT and in the test).

For a given model \( SP \), the exhaustive test set \( \text{Exhaust}_{T}(SP) \) for traces refinement is built by considering all traces of \( SP \) and all their forbidden continuations. We consider the set \( \text{traces}(SP) \) [11], which characterises a trace semantics for \( SP \). We also consider the set \( \text{initials}(SP, t) \) of continuations of the trace \( t \) of \( SP \).

**Definition 3 (Exhaustive test set of \( SP \) for traces refinement).** Given a specification \( SP \), we define \( \text{Exhaust}_{T}(SP) = \{ T_T(t, e) \mid t \in \text{traces}(SP) \land e \not\in \text{initials}(SP, t) \} \).

Exhaustiveness of \( \text{Exhaust}_{T}(SP) \) is formally established by the following theorem, proved in [10].

**Theorem 1 (Exhaustivity of \( \text{Exhaust}_{T} \)).** Given two processes, \( \text{SUT} \) and \( SP \), \( SP \subseteq_T \text{SUT} \) if, and only if \( \forall T_T(s, a) : \text{Exhaust}_{T}(SP); \ t : \text{traces}(\text{Execution}_{\text{SUT}}^{SP}(T_T(s, a))) \bullet \text{last}(t) \neq \text{fail} \)

This extreme test strategy requires the execution of all the traces of \( SP \) with all their forbidden continuations. It yields an inconclusive verdict when a tested trace is not implemented. If there are only \( \text{pass} \) and \( \text{inc} \) verdicts, it guarantees that the SUT refines \( SP \) providing our testability hypotheses hold.

As said above, when selecting a strict subset of \( \text{Exhaust}_{T} \), and running the tests \( T \) of this set as described by \( \text{Execution}_{\text{SUT}}^{SP}(T) \) an element to be covered can be statically covered in the subset, but not covered at runtime. In Section 3, we introduce the notions of exhaustive coverage of an element of the specification, and runtime coverage of this element by the implementation. Before discussing these novel concepts, however, we discuss briefly a symbolic account of the Circus tests.
2.3. Symbolic tests in Circus

The testing theory described above was first cast in the context of CSP [10], rather than Circus. The main difference between Circus and CSP, however, is the added possibility of specifying complex data types using the predicative style of pre and postconditions. Since Circus processes encapsulate the data, it is not surprising that tests can be constructed from a Circus process in the same way as from a CSP process. With similar notions of traces and trace refinement, all results of the CSP theory are maintained.

On the other hand, it is possible and, of interest, to take into account the data operations of a model when specifying a testing strategy. To this end, we have developed a symbolic characterisation of tests and exhaustive test sets for Circus [13]. It is based on the Circus operational semantics, which maintains a symbolic account of the state of a process. We give a brief description of the main definitions here.

The Circus operational semantics defines a transition relation \( p_1 \rightarrow p_2 \) between texts \( p_1 \) and \( p_2 \) of processes. When \( p_1 \xrightarrow{l} p_2 \) holds, we say that there is a transition from \( p_1 \) to \( p_2 \) with label \( l \). We use the typewriter font to distinguish texts (of processes, actions, predicates, and so on), from the entities that they denote. If the label is \( \epsilon \), the execution of the process \( p_1 \) can evolve silently (without any interaction with the environment), so that we then have an execution of \( p_2 \). On the other hand, there may be a label \( d.w \), representing a communication over the channel \( d \) of a value represented by the symbolic variable \( w \). In this case, the execution of \( p_1 \) evolves to that of \( p_2 \), after engaging in the communication \( d.w \).

The definition of this transition relation for processes is based on a transition relation for configurations involving actions. They are triples \( (c \mid s \models A) \) where \( c \) is a constraint over the symbolic variables in use, \( s \) is an assignment to the Circus variables in scope of values represented by symbolic variables, and \( A \) is the text of a Circus action. The symbolic variables constrained in \( c \) are those used in labels \( d.w \) to represent communications and those used in the definition of the state \( s \) to represent values of Circus variables.

To construct symbolic tests, we use the notion of constrained symbolic traces of a process. A constrained symbolic trace is a pair formed by a symbolic trace \( st \) and a constraint \( c \). A symbolic trace is a finite sequence of symbolic events \( d.a_0 \), where \( d \) is a channel, and \( a_0 \) is a symbolic variable that represents the value communicated. The constraint \( c \) is the text of a predicate over the symbolic variables used in \( st \).

Example 3. For the Protocol process, we have the constrained symbolic trace \( ((\text{in}\alpha, \text{out}\beta, \text{in}\gamma), \alpha = \beta) \), for example. It represents all traces where the first input and output values \( \alpha \) and \( \beta \) are the same, and then a new, unconstrained value \( \gamma \) is input. The trace in Example 1 is one of its instances.

We define below the function \( \text{cstraces} \) that characterises the set of constrained symbolic traces of a process. It is parametrised by an alphabet \( a \), which fixes the symbolic variables that can be used in the symbolic trace, and the order in which they can be used. For a process \( \text{begin state} [x : T] \bullet A \text{ end} \), the constrained symbolic traces are those of its main action \( A \), starting from a state in which the state \( x \) takes the value \( w_0 \) constrained by \( w_0 \in T \). This is the set \( \text{cstraces}^a(w_0 \in T, x := w_0, A) \) defined using the operational semantics.

Definition 4.

\[
\begin{align*}
\text{cstraces}^a(\text{begin state}[x : T] \bullet A \text{ end}) &= \text{cstraces}^a(w_0 \in T, x := w_0, A) \\
\text{cstraces}^a(c_1, s_1, A_1) &= \left\{ \begin{array}{l}
st, c_2, s_2, A_2 \mid \text{ast} \leq a \land (c_1 \mid s_1 \models A_1) \xrightarrow{s_2} (c_2 \mid s_2 \models A_2) \\
\bullet \mathcal{R}(st, c_2) \end{array} \right\}
\end{align*}
\]

In defining \( \text{cstraces}^a(c_1, s_1, A_1) \), we consider the configurations \( (c_2 \mid s_2 \models A_2) \) that can be reached by evaluation of the operational semantics from the configuration \( (c_1 \mid s_1 \models A_1) \) identified by the parameters. They are characterised by the transition relation \( (c_1 \mid s_1 \models A_1) \xrightarrow{s_2} (c_2 \mid s_2 \models A_2) \), which is annotated with a trace \( st \). This transition relation is defined in terms of the operational semantics in the usual way.

The symbolic trace \( st \) records the events that arise from the evaluation of \( (c_1 \mid s_1 \models A_1) \) in reaching \( (c_2 \mid s_2 \models A_2) \) as illustrated in Example 3. With \( \text{ast} \leq a \), we require that the symbolic variables used to define \( st \), like \( \alpha, \beta \) and \( \gamma \) in Example 3, are those of the alphabet \( a \), in the order in which they appear in \( a \). We use \( \text{ast} \) to refer to the sequence of variables used in \( st \), and \( \text{ast} \leq a \) requires that it is a prefix of \( a \).
The constraint $c_2$ associated with $st$, however, includes constraints on symbolic variables that are not used in $st$, but are used to represent internal values arising from the evaluation of $(c_1 | s_1 \models A_1)$. These symbolic variables should not be mentioned in the constrained symbolic trace. Above, we use the function $R$ defined below to remove them. When applied to a trace $(st, c)$, it quantifies away every variable in the set $\alpha_c$ of free variables of $c$ that is not in the set $\alpha_{st}$ of symbolic variables used in $st$.

**Definition 5.** For every $(st, c)$, we define $R(st, c)$ as follows.

$$R(st, c) = (st, \exists (\alpha_c \setminus \alpha_{st}) \cdot c)$$

The operational semantics guarantees that all configurations have satisfiable constraints. Therefore, every
constrained symbolic trace is feasible, in the sense that it has at least one valid instance, and so it is guaranteed that the constraint $c_2$ to which $R$ is applied in Definition 4 is satisfiable.

As said above, to construct tests, we also need forbidden continuations. In the symbolic approach, we use symbolic events: pairs formed by a symbolic event and a constraint. A symbolic event is itself formed by a channel name and a symbolic variable. We define the set $csinitials$ of constrained symbolic events over the alphabet $\alpha$ that represent the events that are not initials of $\mathcal{P}$ for any of the instances of its symbolic trace $(st, c)$. A definition of this set is in [13], and its use for test generation is detailed in [20].

**Example 4.** The set $csinitials^\delta (\text{Protocol}, ((\text{in}.\alpha, \text{out}.\beta, \text{in}.\gamma), \alpha = \beta))$ of constrained symbolic events for Protocol after the trace in Example 3, where $\alpha$ is the alphabet $(\alpha, \beta, \gamma, \delta, \ldots)$. It determines that the value $\delta$ output after an input $\text{in}.\gamma$ is different from $\gamma$. We observe that the constraint is over the variable used in the symbolic event, as well as the variables used in the symbolic trace that lead to it. In this example, the constraint refers to $\alpha$, $\beta$, and $\gamma$, as well as $\delta$. □

From the symbolic traces and events, we can construct symbolic tests in the expected way. For a constrained symbolic trace $(st, c_1)$ and a symbolic event $(d_0, c_2)$ that represents a forbidden continuation, the corresponding symbolic test is given by $ST_T^c((st, c_1), (d_0, c_2))$ defined below.

**Definition 6.**

$$ ST_T^c((\langle \rangle, c_1), (d_0, c_2)) = \text{pass} \rightarrow d? \beta_0 : c_2 \rightarrow \text{fail} \rightarrow \text{Stop} $$

$$ ST_T^c((d_{st}.\alpha_0) \cap st, c_1), (d_0, c_2)) = \text{inc} \rightarrow d_{st}.? \alpha_0 : (\exists \alpha \in \alpha_0 \bullet c_1) \rightarrow ST_T^c(st, c_1), (d_0, c_2)) $$

For a constrained symbolic trace $(\langle \rangle, c_1)$ whose symbolic trace is empty, we only add to the test the verdict event $\text{pass}$. After that, corresponding to a symbolic forbidden continuation $(d_0, c_2)$, we have an input communication $d? \beta_0 : c_2$, which accepts an input $\beta_0$ through the channel $d$, with the constraint $c_2$ restricting the accepted values of the variable $\beta_0$. Similarly, for the prefixings corresponding to each of the symbolic events $d_{st}.\alpha_0$ of the symbolic trace $st$, we use the constraint $c_1$ to extract the right constraint over the input $\alpha_0$. The $\alpha$ parameter of $ST_T$ records the symbolic variables already used, and the constraint on $\alpha_0$ is obtained by quantifying all variables not in $\alpha$ and different from $\alpha_0$, namely, those in the list $\alpha_0$.

The instantiation of a symbolic test is defined below as a function that yields a set of concrete tests.

**Definition 7.**

$$ \text{instTest} (\text{Stop}) = \{ \text{Stop} \} $$

$$ \text{instTest}(d \rightarrow A) = \{ TA : \text{instTest} (A) \bullet d \rightarrow TA \} $$

$$ \text{instTest}(d? \alpha_0 : c \rightarrow A) = \{ v_0, TA \mid c[v_0/\alpha_0] \land TA \in \text{instTest}(A[v_0/\alpha_0]) \bullet d, v_0 \rightarrow TA \} $$

The instances of a symbolic test are built in the following way. The action $\text{Stop}$ is not really symbolic; its only instance is itself. For a prefixing $d \rightarrow A$, whose communication is a simple synchronisation like $\text{inc}$, $\text{pass}$, or $\text{fail}$, for example, the instances are prefixing formed out of $d$ itself and the instances $TA$ of the prefixed action $A$. Finally, if we have a prefixing $d? \alpha_0 : c \rightarrow A$, then the instances consider all possible ways of choosing for communication a value $v_0$ that satisfies the constraint $c$, and the corresponding instances of the action $A[v_0/\alpha_0]$, where the choice of $v_0$ for $\alpha_0$ is recorded.

**Example 5.** For the constrained symbolic trace and forbidden continuation in Example 4, we get the following symbolic test.

$$ \text{inc} \rightarrow \text{in}.\alpha : \text{true} \rightarrow \text{inc} \rightarrow \text{out}.\beta : \alpha = \beta \rightarrow \text{inc} \rightarrow \text{in}.\gamma : \alpha = \beta \rightarrow \text{pass} $$

$$ \text{out}.\delta : \alpha = \beta \land \gamma \neq \delta \rightarrow \text{fail} \rightarrow \text{Stop} $$

The test in Example 2 is an instance of this test. □
A slightly different definition of instantiation that avoids the enumeration of all the instances of the final forbidden symbolic events is possible: given a symbolic test constructed from the constrained symbolic trace \((st, c_1)\) followed by the forbidden constrained symbolic event \((d_0, c_2)\), the variables in \((st, c_1)\) are instantiated with values that satisfy the constraint \(c_1\), and these instantiations are propagated to \(c_2\) as described above, but the final constraint is not instantiated. In this case, instances of symbolic tests are Circus processes where the single constrained symbolic event in the symbolic test is used in a final synchronisation with a predicate. Such an instance of the symbolic test of Example 5 is as follows.

\[
\text{inc} \rightarrow \text{in.0} \rightarrow \text{inc} \rightarrow \text{out.0} \rightarrow \text{inc} \rightarrow \text{in.1} \rightarrow \text{pass} \rightarrow \text{out.} \delta : 1 \neq \delta \rightarrow \text{fail} \rightarrow \text{Stop}
\]

A symbolic exhaustive test set is just a set of symbolic tests. Selection strategies based on symbolic tests are the subject of Section 3, selection of instances is addressed in Section 3.4, and further selection focused on coverage of synchronisations in Circus model is studied in Section 4.5.

3. Selection and traces refinement

The criteria for selecting a subset of the generally infinite set of possible tests are the core of any testing strategy. This can be achieved via coverage criteria, test purposes, uniformity or regularity hypotheses, or more generally some property of tests [28]. In the testing theory for CSP and Circus, tests are built from traces of the specification and a forbidden continuation; the exhaustive test set covers all these traces and events. So, selection must ultimately define a subset of the set of traces and their forbidden continuations.

As already mentioned, when the considered conformance relation is traces refinement, it is acceptable that a trace of the specification is not implemented in the SUT. As seen in Section 2.2, in this case execution of the corresponding test yields an inconclusive verdict. Thus it may be the case that a selected test is not executable, and if there is another test that may be able to fulfill the selection criterion, it must be executed, and we should proceed in this way, until either a satisfactory test is executed or it is certain that none exists. This has an impact on the way in which test selection for traces refinement can be defined and applied.

There are two main interrelated tasks involved in the definition of a selection strategy for traces refinement: a (formal) definition of (a) the (possibly still infinite) subset of all those tests that can contribute to the fulfillment of the selection criterion and (b) a test driver. We explain in the next section why defining an exhaustive test set with respect to the selection criteria is useful when considering traces refinement.

Whether concrete or symbolic tests are considered is irrelevant for definition of the exhaustive test set. We just observe that the notion of constrained symbolic traces, which is central in the Circus testing theory, is well suited for the definition of uniformity subdomains in the selection of both traces and initials: the constraints of the symbolic traces and events can be reused. On the other hand, we need to construct a driver of concrete tests. When selection is based on symbolic tests, we have, in addition, to address the fact that it may be the case that not all instantiations of a selected symbolic test are executable by the SUT.

Next, we illustrate the problem of selection for traces refinement. In Section 3.2, we consider several approaches to the definition of an exhaustive test set and of a test driver with respect to various selection criteria. In Section 3.3, we address factorisation of tests as for adaptive testing [33], and briefly discuss online and offline test generation. Section 3.4 discusses symbolic tests. Finally, Section 3.5 considers the issues related to the finiteness of the exhaustive test sets with respect to the given criteria.

3.1. The problem

To explain the problem associated with test selection for traces refinement in detail, we consider the case where the selection is based on a coverage criterion, that is, a set of elements of the specification are required to be exercised by at least one test experiment. The elements may be, for example, synchronisation events, pairs of related events, or more sophisticated requirements on execution traces.

If the test set is selected in a static way, it may turn out that the test selected to ensure coverage of a given element reaches an inconclusive verdict before executing it because the trace is not implemented. It may be the case, however, that other traces that provide coverage are implemented and that covering it is achievable in the SUT. Thus it is necessary to select and design tests that try at runtime other ways of covering this element, in order to ensure that if it is executable by the SUT, then it is exercised.
We define below a test driver that runs all these tests until a pass verdict, possibly followed by a fail verdict.

Example 6. For simplicity, we consider channels $a, b, c, d$ and $e$ that are used for synchronisation, but do not communicate any value. In this case, the constrained symbolic traces degenerate to standard traces, because there is no need to introduce symbolic variables to represent communicated values, and the only valid constraint is just true. In addition, we consider a stateless Circus process $P$ defined below.

$$P \triangleq \begin{array}{c}
\text{begin} \bullet a \rightarrow e \rightarrow c \rightarrow \text{Skip} \cap \\
b \rightarrow e \rightarrow d \rightarrow \text{Skip} 
\end{array}$$

In what follows, whenever we present a stateless process like this, for brevity, we omit the begin and end keywords and identify the process with its action after the ‘$\bullet$’.

Some of the processes that trace-refine $P$ are $P$ itself and processes whose main actions are either of the actions in the internal choice. A test set that covers the event $e$, for instance, is the singleton including the process whose action is $\text{inc} \rightarrow a \rightarrow e \rightarrow \text{pass} \rightarrow d \rightarrow \text{fail} \rightarrow \text{Stop}$. To be sure, however, that if a trace covering $e$ exists in the SUT, then $e$ is covered by some test experiment, we need to identify the set of all tests that provide the required coverage and use a new way of driving these tests. Alternatively, a new form of test may be used, which adapts at runtime to the SUT.

The first solution is to design a driver based on a set of all tests covering $e$ that will trigger their executions until $e$ is exercised. The second solution is to have tree-shaped tests such as:

$$\begin{array}{c}
\text{inc} \\
\rightarrow \quad \left( \\
\begin{array}{c}
\square \\
b \rightarrow \text{inc} \rightarrow e \rightarrow \text{pass} \rightarrow c \rightarrow \text{fail} \rightarrow \text{Stop} \\
\end{array} \right)
\end{array}$$

This test offers to the SUT the choice between two traces of the specification that pass through $e$. With this test, if the SUT is deterministic, if there exists in the SUT a specified trace exercising $e$, it is executed. When the SUT is not deterministic, by applying the test a sufficient number of times, under the complete test assumption, we know that the trace is executed. If there is no such trace, the test is inconclusive. \(\square\)

In the next section we explore both solutions indicated in the above example.

3.2. A solution: monitoring runtime coverage

As said above, when combining test selection and traces refinement, use of a selection criterion requires both the selection of traces and forbidden continuations and the design of a driver that ensures that the criterion is fulfilled at runtime, if possible. We proceed by selecting all the tests that satisfy the criterion, and define the corresponding driver that tries all these tests if necessary until a test is successfully completed.

Example 7. For illustration, we consider as selection criterion coverage of a particular event $e$. In this case, given a specification $SP$, the exhaustive set of tests that satisfy the selection criterion is as follows.

$$\text{Exhaust}_T(SP) |_e = \{ T(t, a) \mid t \in \text{traces}(SP) \land t|_e \neq () \land a \notin \text{initials}(SP, t) \}$$

where $t|_e$ eliminates from $t$ all events different from $e$. This subset of $\text{Exhaust}_T(SP)$ covers all the traces where $e$ occurs at least once. For Example 6, the tests in this set are as follows.

$$\begin{array}{c}
a \rightarrow \text{inc} \rightarrow e \rightarrow \text{pass} \rightarrow a \rightarrow \text{fail} \rightarrow \text{Stop} \\
a \rightarrow \text{inc} \rightarrow e \rightarrow \text{pass} \rightarrow b \rightarrow \text{fail} \rightarrow \text{Stop} \\
a \rightarrow \text{inc} \rightarrow e \rightarrow \text{pass} \rightarrow d \rightarrow \text{fail} \rightarrow \text{Stop} \\
a \rightarrow \text{inc} \rightarrow e \rightarrow \text{inc} \rightarrow c \rightarrow \text{pass} \rightarrow a \rightarrow \text{fail} \rightarrow \text{Stop} \\
a \rightarrow \text{inc} \rightarrow e \rightarrow \text{inc} \rightarrow c \rightarrow \text{pass} \rightarrow b \rightarrow \text{fail} \rightarrow \text{Stop} \\
\ldots \\
b \rightarrow \text{inc} \rightarrow e \rightarrow \text{pass} \rightarrow a \rightarrow \text{fail} \rightarrow \text{Stop} \\
b \rightarrow \text{inc} \rightarrow e \rightarrow \text{pass} \rightarrow b \rightarrow \text{fail} \rightarrow \text{Stop} \\
b \rightarrow \text{inc} \rightarrow e \rightarrow \text{pass} \rightarrow c \rightarrow \text{fail} \rightarrow \text{Stop} \\
b \rightarrow \text{inc} \rightarrow e \rightarrow \text{inc} \rightarrow d \rightarrow \text{pass} \rightarrow a \rightarrow \text{fail} \rightarrow \text{Stop} \\
\ldots
\end{array}$$

We define below a test driver that runs all these tests until a pass verdict, possibly followed by a fail verdict.
is observed. This is ensured by a test monitor process $T_{\text{Monitor}}$ executed alongside the tests.

$$\text{Driver}(SP, SUT) |_e = (\| T : \text{Exhaust}_T(SP) |_e \rightarrow \text{Execution}^{SP}_{SUT}(T) \| [\{inc, pass, fail\}] ) \text{ TMonitor}$$

where

$$T_{\text{Monitor}} = inc \rightarrow T_{\text{Monitor}} \Box pass \rightarrow fail \rightarrow \text{Stop}$$

Running $\text{Driver}(SP, SUT) |_e$ ensures that if $e$ is executable by the SUT, it is covered at runtime. This means that some test based on a trace where $e$ occurs reaches a conclusive verdict: pass or fail. (If the SUT is nondeterministic, the driver needs to be executed several times, and we need to rely on the complete test assumption.) The tests are executed in interleaving (in parallel independently) until one of them reaches a pass event. In this case, we either have an immediate deadlock, or just the associated forbidden continuation as an internal event of the test execution, followed by an observable fail. We recall that all events of the specification are internal to a test execution, and so not visible to the $T_{\text{Monitor}}$ process.

A shortcoming of the above driver is that it makes an implicit arbitrary selection of a forbidden continuation. A more liberal $T_{\text{Monitor}}$ should allow all (or specific) forbidden continuations to be tested.

If $e$ is not covered at runtime with the strategy above, all the tests return an inconclusive verdict. On the other hand, the fact that all tests return an inconclusive verdict does not mean that $e$ has not been executed since some of the tests may return an inconclusive verdict after having exercised $e$.

Selection of tests is often based on a given property $\pi$ of traces or tests. Examples of such properties are coverage of an event, as considered above, or absence of a particular subsequence of events, and so on. In this case, it is usual to consider as selection criteria either: at least one test satisfying $\pi$ is executed, or all the tests satisfying $\pi$ are executed. We call the former existential selection of tests with respect to $\pi$, and the latter universal selection with respect to $\pi$. We can imagine, of course, some intermediate criteria where several of these tests are selected, or some different criterion that corresponds to a global property of the set of selected tests. As explained later on, however, these selection criteria can be addressed using compositions and variations of the definitions we describe below.

Properties of traces, rather than tests, may also be considered for selection criteria. In what follows, we first discuss existential or universal selection of traces and, in this case, the fact that there are several tests for one trace must be taken into account. Afterwards, we discuss selection based on properties of tests, and consider existential and universal selection as informally discussed above. We observe that the problem discussed in the previous section, which arises from non-implemented traces of the specification, is only an issue for existential selection (of either traces of tests) and its variants.

To characterise the criteria based on properties of traces, we note that for each trace $t$ of a specification $SP$, we have the set of tests $\text{AllTests}_T(t, SP)$ defined below.

$$\text{AllTests}_T(t, SP) = \{ T_T(t, e) | e \notin \text{initials}(SP, t) \}$$

It contains all tests built from $t$ and one of its forbidden continuations $e$.

For a property $\pi$ of traces, we have the possible selection criteria below.

**existential selection of traces:** there is at least one trace $t$ satisfying $\pi$, such that, $\text{AllTests}_T(t, SP)$, the test set identified by $t$ is executed (that is, all tests in $\text{AllTests}_T(t, SP)$ are executed); or

**universal selection of traces:** for all implemented traces $t$ satisfying $\pi$, $\text{AllTests}_T(t, SP)$ is executed.

Moreover, several properties $\pi_1, \ldots, \pi_n$ of traces may be considered; the coverage of a set of elements is an example. In such cases, one may require either of the following criteria.

**multiple existential selection of traces:** for every $\pi_i$, there is at least one trace $t$ satisfying $\pi_i$, such that $\text{AllTests}_T(t, SP)$ is actually executed; or

**multiple universal selection of traces:** for every $\pi_i$, for every implemented trace $t$ satisfying $\pi_i$, the set $\text{AllTests}_T(p, SP)$ is executed.
Coming back to test selection, for a given property $\pi$ of tests, one may require either of the following.

**Existential selection of tests:** there is at least one test $T$ satisfying $\pi$, that is actually executed, if there is one that is implemented, or

**Universal selection of tests:** all implemented tests $T$ satisfying $\pi$ are executed.

Direct test selection makes it possible to focus on specific forbidden continuations, for instance to consider only some specific forbidden event. The property $\pi$ may also combine requirements on the traces and the forbidden continuations, like in, for instance, “all the tests with a trace $t$ where event $e_1$ occurs and event $e_2$ is the forbidden continuation”. In Example 7, for instance, such a criterion for test selection allows us to restrict the set of relevant tests to those that have $a$, for example, as a forbidden continuation. In this case, only three of the tests enumerated in Example 7 are retained for testing. Multiple existential and universal selection criteria for tests can be tackled in the same way as those for traces. Below, we consider exhaustive test sets and drivers for each of the above classes of traces and tests selection criteria.

### 3.2.1. Existential selection of traces

For existential selection, the selected test set $\text{Existential}_{t}^{\text{trace}}(SP)|_{\pi}$ needs to be structured as a set of test sets characterised by $\text{AllTests}_{T}$, as defined below.

$$\text{Existential}_{t}^{\text{trace}}(SP)|_{\pi} = \{\text{AllTests}_{T}(t, SP) \mid t \in \text{traces}(SP) \land t \models \pi\}$$

We use the notation $t \models \pi$ to indicate that the trace $t$ satisfies the property $\pi$.

The execution of all the tests associated with an implemented trace $t$ is specified below as a simple driver that runs independently and to conclusion all tests in $\text{AllTests}_{T}(t, SP)$.

$$\begin{array}{c}
\text{TSMonitor} = \text{done} \rightarrow \text{Stop} \sqcap \text{inc} \rightarrow \text{Stop} \\
\text{Run} \rightarrow \text{pass} \rightarrow \text{Run} \sqcap \text{pass} \rightarrow \text{Run} \rightarrow \text{Run}
\end{array}$$

A driver that ensures existential coverage can be specified as follows: independently, for each trace $t$ that defines a set of tests $\text{AllTests}_{T}(t, SP)$ in $\text{Existential}_{T}^{\text{trace}}(SP)|_{\pi}$, the driver above is run under the control of a monitor that observes whether a pass event takes place. When it does, it means that $t$ is implemented. The monitor continues the execution of the other tests based on $t$, and sends to the other drivers for the other traces a done event to make them to stop. Formally, we have the following definition for a generic driver, for a specification $SP$ and some property $\pi$ of a trace.

$$\text{ExistDriver}_{t}^{\text{trace}}(SP, SUT)|_{\pi} =$$

$$\left(\\left[\\left[\\left[\text{done}\right]\right]\right]\right)\ \text{TSMonitor} \left.\left(\text{TS : Existential}_{t}^{\text{trace}}(SP) \mid_{\pi}\bullet\right)\right.\right.$$  

$$\left(\\left[\\left[\\left[\text{TSMonitor} \left.\left(\text{T : TS \bullet Execution}_{SUT}^{SP}(T)\right)\right]\right]\right]\right]\left[\\left[\\left[\text{inc, pass, fail}\right]\right]\right]\right)$$

where $\text{TSMonitor}$ is below. It stops when a done occurs, and raises a done event when a pass occurs.

$$\text{TSMonitor} = \text{done} \rightarrow \text{Stop} \sqcap \text{inc} \rightarrow \text{TSMonitor} \sqcap \text{pass} \rightarrow \text{done} \rightarrow \text{Run}$$

Run just continues running the other tests based on the same trace.

$$\text{Run} = \text{inc} \rightarrow \text{Run} \sqcap \text{pass} \rightarrow \text{Run} \sqcap \text{pass} \rightarrow \text{Run}$$

In the definition above of $\text{ExistDriver}_{t}^{\text{trace}}(SP)|_{\pi}$, each of the sets $\text{TS}$ in $\text{Existential}_{T}^{\text{trace}}(SP)|_{\pi}$ is considered. The drivers for each of these sets are run in parallel, synchronising on the event done. Each driver runs all tests $T$ in $\text{TS}$ independently, but under the control of $\text{TSMonitor}$, which observes done as well as the verdict events. If a done event occurs, $\text{TSMonitor}$ stops (and so the tests under its control stop), because this indicates that a monitor for another test set has observed a test with a conclusive verdict. Otherwise, $\text{TSMonitor}$ and its tests proceed until a pass is observed, when done is raised, but the controlled tests proceed to conclusion: Run just ignores all verdict events. The done event is local to the existential driver; it is used only for synchronisation between the monitors of the tests associated with each trace $t$. Termination of the driver depends of the size of the set of selected tests. This is further discussed in Section 3.5.
Example 8. Coming back to coverage of an event $e$ considered in Example 7, we have:

$$\text{Existential}_{T}^{\text{trace}}(SP)|_{(t,\neq(\cdot))} = \{ \text{AllTests}_{T}(t, SP) \mid t \in \text{traces}(SP) \land t \vdash e \neq \langle \rangle \}$$

The distributed union of the test sets in this set is exactly $\text{Exhaust}_{T}(SP)|_{e}$. Here, their grouping based on the traces $t$ as defined by $\text{AllTests}_{T}(t, SP)$ allows us to consider the alternative driver below.

$$\text{ExistDriver}_{T}^{\text{trace}}(SP, SUT)|_{(t,\neq(\cdot))} = \left( \begin{array}{c} \left\{ \text{TS} : \text{Existential}_{T}^{\text{trace}}(SP)|_{(t,\neq(\cdot))} \right\} \\ \left( \begin{array}{c} T : \text{Execution}_{SUT}^{SP}(T) \\ \text{inc}, \text{pass}, \text{fail} \\ \text{TSMonitor} \end{array} \right) \end{array} \right) \setminus \left\{ \text{done} \right\}$$

This driver ensures that for at least one implemented trace covering $e$, if there is one, all the tests are executed, that is, all the forbidden events are attempted. As already said, the driver $\text{Driver}(SP, SUT) \vdash e$ presented in Example 7 attempts only one of them chosen arbitrarily.

As usual, if the SUT is nondeterministic, coverage has to rely on the complete test assumption and on running the driver several times. This is the case for all drivers that we present.

3.2.2. Universal selection of traces

The case of universal selection is easier to formalise; there is no need to consider a set of test sets as in the previous section. The test set to be considered is as follows.

$$\text{Universal}_{T}^{\text{trace}}(SP)|_{e} = \{ T_{T}(t, a) \mid t \in \text{traces}(SP) \land t \vdash \pi \land a \not\in \text{initials}(SP, t) \}$$

All tests that are implemented must be run, so the driver attempts to execute all tests.

$$\text{UnivDriver}_{T}^{\text{trace}}(SP, SUT)|_{e} = \left\{ T : \text{Universal}_{T}^{\text{trace}}(SP)|_{e} \bullet \text{Execution}_{SUT}^{SP}(T) \right\}$$

Example 9. Coming back again to coverage of an event $e$, we have

$$\text{Exhaust}_{T}(SP)|_{e} = \text{Universal}_{T}^{\text{trace}}(SP)|_{(t,\neq(\cdot))}$$

The corresponding driver $\text{UnivDriver}_{T}^{\text{trace}}(SP, SUT)|_{(s,\neq(\cdot))}$ executes all tests arising from all traces that include at least one occurrence of $e$. The driver $\text{Driver}(SP, SUT)$ in Example 7 executes only one of these tests for each trace with at least one occurrence of $e$.

3.2.3. Multiple existential or universal selection of traces

Selection criteria based on a set of properties $\Pi = \{ \pi_{1}, \ldots, \pi_{n} \}$ can be handled by considering the test sets and the drivers corresponding to each property $\pi_{i}$. For multiple existential coverage of traces, we have a set of test sets for each $\pi_{i}$, and the driver executes independently each of the existential drivers.

$$\text{MExistDriver}_{T}^{\text{trace}}(SP, SUT)|_{\Pi} = \left\{ \pi_{i} : \Pi \bullet \text{ExistDriver}_{T}^{\text{trace}}(SP, SUT)|_{\pi_{i}} \right\}$$

Example 10. A classical example of a multiple existential selection criteria is that every event must be covered at least once. For a set $E$ of events, we have the following driver:

$$\text{MExistDriver}_{T}^{\text{trace}}(SP, SUT) \vdash E = \left\{ e : E \bullet \text{ExistDriver}_{T}^{\text{trace}}(SP, SUT)|_{e} \right\}$$

For multiple universal selection criteria, we can consider a test set containing all tests obtained for each property $\pi_{i}$. There is no need to keep separate sets of tests, since they are all to be executed. We can, therefore, use a driver similar to $\text{UnivDriver}_{T}^{\text{trace}}(SP, SUT)|_{\pi}$ previously presented.
3.2.4. Existential or universal selection of tests

For a given property $\pi$ of tests, we consider, for both existential and universal selection, the following exhaustive test set. We use $T \vdash \pi$ to denote the fact that the test $T$ satisfies $\pi$.

$$\text{Exhaust}^\text{test}_T(SP) \mid \pi = \{ T : \text{Exhaust}_T(SP) \mid T \vdash \pi \}$$

There is no need to use a set of test sets like we have done for existential selection of traces.

For existential selection of the tests satisfying $\pi$, the driver is as follows.

$$\text{ExistDriver}^\text{test}(SP, SUT) \mid \pi = (\| T : \text{Exhaust}^\text{test}_T(SP) \mid \pi \bullet \text{Execution}^S_{\text{SUT}}(T)\| [\| \text{inc, pass, fail} \| ]) \text{TMonitor}$$

where $\text{TMonitor}$ is as in Example 7.

$$\text{TMonitor} = \text{inc} \rightarrow \text{TMonitor} \boxdot \text{pass} \rightarrow \text{fail} \rightarrow \text{Stop}$$

For universal selection of tests satisfying $\pi$, the driver is shown below.

$$\text{UnivDriver}^\text{test}(SP, SUT) \mid \pi = \| T : \text{Exhaust}^\text{test}_T(SP) \mid \pi \bullet \text{Execution}^S_{\text{SUT}}(T)\|$$

This is exactly the same driver used for universal selection based on traces, except that it uses the tests in $\text{Exhaust}^\text{test}_T(SP) \mid \pi$ (rather than those in $\text{Exhaust}^\text{trace}_T(SP) \mid \pi$).

To give an example, we define below the process $\text{end}_T(T)$; it captures the final behaviour of a test $T$, where, after signalling a pass, it attempts to execute a forbidden continuation.

Definition 8.

$$\text{end}_T(\text{pass} \rightarrow P) = P \quad \text{end}_T(\text{inc} \rightarrow e \rightarrow P) = \text{end}_T(P)$$

This definition is used in the next example and in the next section.

Example 11. One may consider the universal selection criterion “all the tests where a given event $e$ is a forbidden continuation”, possibly because it is especially critical not to execute this event $e$ when it is forbidden by the specification. In this case, the test set is as follows.

$$\text{Exhaust}^\text{test}_T(SP) \mid _e = \{ T : \text{Exhaust}_T(SP) \mid \text{end}(T) = e \rightarrow \text{fail} \rightarrow \text{Stop} \}$$

More imaginative selection criteria can be dealt with by the definition of adequate test sets or sets of test sets, or by composition of drivers. We have considered the main kinds of selection strategies, and shown how to construct the corresponding exhaustive test set for the required selection criteria and accompanying driver. We cannot claim to have explored every conceivable criterion, but note that driver composition with exchanges of messages, as done for existential selection, can cater for quite a wide range of selection strategies. If needed, it is possible to specify in Circus drivers that use, for example, counters and guards.

3.3. Factorisation

As already said, instead of using a monitor process to define special drivers, it is possible to factorise the tests in the exhaustive test set to define a single tree-shaped test as it is done for adaptive testing in [33]. This test offers the choice between all the tests selected; the second test in Example 6 illustrates the idea.

Factorisation decreases the number of inconclusive verdicts, since it gives the SUT the choice of several continuations available in the test set. Factorised tests have, however, a difficulty concerning coverage of behaviours, since the choices are no more under the control of the test and can be biased by the SUT.
Example 12. We consider, for instance, the factorisation of the following tests.

\[
\begin{align*}
\text{inc} & \rightarrow a \rightarrow \text{pass} \rightarrow d \rightarrow \text{fail} \rightarrow \text{Stop} \\
\text{inc} & \rightarrow a \rightarrow \text{inc} \rightarrow e \rightarrow \text{pass} \rightarrow c \rightarrow \text{fail} \rightarrow \text{Stop}
\end{align*}
\]

It gives the following tree-shaped test.

\[
\begin{align*}
\text{inc} & \rightarrow a \rightarrow (\text{pass} \rightarrow d \rightarrow \text{fail} \rightarrow \text{Stop} \\
& \quad \text{inc} \rightarrow e \rightarrow \text{pass} \rightarrow c \rightarrow \text{fail} \rightarrow \text{Stop})
\end{align*}
\]

After the SUT performs the trace \(\langle a \rangle\), there is a choice between the testing events \(\text{pass}\) and \(\text{inc}\) that is left up not to the test, but to the environment of the test execution. It is an external choice over events that are not in the alphabet of the SUT.

For the non-factorised tests, the environment of a test execution can be a simple process that is prepared to accept interaction on any of the events \(\text{inc}, \text{pass},\) and \(\text{fail}\), at any moment. Even in such a liberal environment, it is guaranteed that the interaction with the SUT defined by the trace that corresponds to the test is attempted in the test execution. If the test is factorised, though, the environment of the test execution is offered choices between \(\text{pass}\) and \(\text{inc}\) events, whenever there is a possibility, according to the specification, of extending the trace or deadlocking. To ensure coverage, both choices should be tried.

A related concern arises when there are several possibilities of failure.

Example 13. We consider, for instance, the factorisation of the following tests.

\[
\begin{align*}
\text{inc} & \rightarrow a \rightarrow \text{pass} \rightarrow d \rightarrow \text{fail} \rightarrow \text{Stop} \\
\text{inc} & \rightarrow a \rightarrow \text{pass} \rightarrow e \rightarrow \text{fail} \rightarrow \text{Stop}
\end{align*}
\]

It gives the following tree-shaped test.

\[
\begin{align*}
\text{inc} & \rightarrow a \rightarrow \text{pass} \rightarrow (\text{d} \rightarrow \text{fail} \rightarrow \text{Stop} \\
& \quad \text{e} \rightarrow \text{fail} \rightarrow \text{Stop})
\end{align*}
\]

In this case, after the occurrence of \(a\), if the environment of the test execution chooses to synchronise on \(\text{pass}\), it then has no control over the choice between \(d\) and \(e\): these events are not in its alphabet. The test is not making a choice, but rather offering it to the SUT. If the SUT can perform any of them, the mistake is going to be detected, but it is not possible to determine which of the mistaken events are possible, since the SUT is not forced to perform any of them.

It remains, however, that the SUT drives the test by making the (external) choices of model events offered in the test. Since just one path of the tree-shaped test is executed in a test experiment, we have an existential selection (by the SUT) of a test combined into the tree. Moreover, only the complete test assumption and enough executions of the tree-shaped test can guarantee that all paths in the tree-shaped test (and, therefore, all tests combined in the tree) are executed.

We define below a function \(\text{Fact}^{SP}(TS)\) that defines the factorised tree-shaped tests coming from a test set \(TS\). It is defined in terms of a function \(\text{FactP}^{SP}(TS, t)\), which takes as an extra parameter the path (a trace) \(t\) that defines the branch of the tree-shaped test that is being constructed.

**Definition 9 (Factorisation).**

\[
\text{Fact}^{SP}(TS) = \text{FactP}^{SP}(TS, \langle \rangle)
\]

\[
\text{FactP}^{SP}(TS, t) = \text{TFail}(TS, t) \sqcap \text{TCont}^{SP}(TS, t)
\]
TFail(TS, t) = Stop \quad [\text{if } t \notin \text{trace } TS]\]

TFail(TS, t) = pass \rightarrow T : \{ T : TS \mid \text{trace}_T(T) = t \} \bullet \text{end}_T(T) \quad [\text{if } t \in \text{trace } TS]\]

TCont^{SP}(TS, t) = Stop \quad [\text{if } \text{initials}_T(TS, t) = \emptyset]

TCont^{SP}(TS, t) = inc \rightarrow e : \text{initials}_T(TS, t) \bullet e \rightarrow \text{Fact}^{SP}(TS, t \circ (e)) \quad [\text{if } \text{initials}_T(TS, t) \neq \emptyset]

For any set TS, \text{Fact}^{SP}(TS) is given by \text{Fact}^{SP}(TS, \langle \rangle); initially, just the empty path has been constructed. For any path t, this is an external choice between tests defined by functions TFail(TS, t) and TCont^{SP}(TS, t). With TFail(TS, t), we consider whether t is the trace of a test in TS or not. We define the set trace \{ TS \} of traces of a set of tests TS as the set of specification traces used in its tests, not including the forbidden continuations. We use the relational image operator f \{ S \}; it provides the set of results obtained by applying f to each element in the set S. The trace of a single test T is defined as follows.

**Definition 10.**

\[
\text{trace}_T(pass \rightarrow P) = \langle \rangle \quad \text{trace}_T(inc \rightarrow e \rightarrow P) = (e) \cap \text{trace}_T(P)
\]

If t is not a trace of a test in TS, then TFail(TS, t) is Stop, which is a unit for external choice: \text{Stop} \circ P = P. For example, TS may not have any test for the empty trace \langle \rangle, and in this case TFail(TS, \langle \rangle) does not add anything to the tree-shaped test. On the other hand, if there are tests T in TS whose trace is t, then, for each of them, we add its treatment of the forbidden continuation, characterised by \text{end}_T(T), to the tree.

With TCont^{SP}(TS, t), we consider whether t is the prefix of a trace of a test in TS or not. We use the notion of initials of a test set TS after a trace t formally defined as follows.

**Definition 11.**

\[
\text{initials}_T(TS, t) = \{ e \mid \exists T : TS; s \bullet \text{trace}_T(T) = t \circ (e) \circ s \}
\]

If t has no continuation, then TCont^{SP}(TS, t) is just Stop. Otherwise, we add an intermediary verdict inc followed by a branch (in an external choice) for each of the continuations e.

**Example 14.** The test in Example 6 can be built from the test set including

\[
\text{inc} \rightarrow a \rightarrow \text{inc} \rightarrow e \rightarrow \text{pass} \rightarrow d \rightarrow \text{fail} \rightarrow \text{Stop}
\]

and

\[
\text{inc} \rightarrow b \rightarrow \text{inc} \rightarrow e \rightarrow \text{pass} \rightarrow c \rightarrow \text{fail} \rightarrow \text{Stop}
\]

No special driver is required in this case. \(\square\)

As already indicated above, however, the two approaches discussed here, namely, factorisation and the definition of exhaustive test sets and drivers, are not equivalent. In the execution of a factorised test, the control, exercised via choice of events, is left to the SUT or the test environment. This is in contrast with the drivers in Section 3.2, which control the execution of the tests to which they are associated.

A third approach is to alternate the control between the driver and the SUT, as in on-the-fly testing [58, 59, 32], where test derivation and execution are integrated into a single process. This approach is also called online testing, in contrast with offline testing, where test generation is a separate process that takes places before execution. Online testing is especially relevant when testing reactive systems: the next event of the tester is generated in function of the reaction of the SUT.

In this paper, we have not addressed the issue of generation of the various exhaustive test sets occurring in the drivers: they are defined in an abstract, predicative way. Similarly, the factorisation function above starts from a given subset of the exhaustive test set, and thus is not a generation algorithm. The corresponding
test-generation algorithms from a Circus specification can be developed and used either offline, following the patterns of the drivers defined in Section 3.2, or online.

Online testing would avoid running in parallel all the tests that satisfy the criterion. On the other hand, online testing would require integrating in the driver the generation algorithm of the exhaustive test sets for ensuring that all the relevant tests are attempted until one or all are completed (depending of the kind of considered selection: existential or universal).

### 3.4. Partial implementation of symbolic tests

As explained in Section 2.3, the Circus testing theory offers a symbolic characterisation of the concrete tests and of the exhaustive concrete test set. It is possible to specify a testing strategy for a Circus specification at the concrete level, just following what is presented in Section 3.2 or 3.3. Uniformity hypotheses on instantiations of constrained symbolic tests, however, provide a natural selection criterion. For instance, a simple hypothesis states that the verdict for all instances of a symbolic test is the same. In this case, we assume that the verdict of the test in Example 2 is the same verdict of all instances of the symbolic test in Example 5. Constrained symbolic tests enable the definition of powerful selection strategies that take into account data types properties. We, therefore, consider now how to select from symbolic tests, and then instantiate the selected tests and run them via concrete drivers to ensure runtime coverage.

We have a two-level selection method. Firstly, we need to provide a symbolic exhaustive test set with respect to the selection criteria of interest. Just like in Section 3.2, this amounts to the definition of all those symbolic tests that, when instantiated, may contribute at runtime to the satisfaction of the criterion. In this case, we need to rely on properties of symbolic traces or symbolic tests, but that is all.

Secondly, we need to define drivers for the instantiations of the symbolic tests. The challenge is that, when starting the testing experiments with a given symbolic test, it may be only partially implemented. Moreover, if there is no implemented instantiation, it is necessary to try another symbolic test of the exhaustive test set, and actually all of them until either one concrete test reaches a conclusion, or it is certain that it is impossible to fulfill the criterion for the SUT. Mechanisms similar to those in Section 3.2 must be used for existential or universal selection among those concrete tests corresponding to a symbolic test.

The execution of all the implemented instances of a given symbolic test $ST$ is specified as follows.

$$UnivInstDriver(ST, SP, SUT) = \{ T : instTest(ST) \cdot Execution_{SUT}^{SP}(T) \}$$

As said above, however, symbolic tests are generally used to select only one of their instantiations. The execution of at least one implemented instance of a symbolic test $ST$, if there is one, is specified below.

$$ExistInstDriver(ST, SP, SUT) = (\{ T : instTest(ST) \cdot Execution_{SUT}^{SP}(T) \} \{ inc, pass, fail \} TMonitor)$$

This is similar to the existential selection driver addressed in Section 3.2, but we monitor tests coming from a single test set, namely, the set of instantiations of the symbolic test $ST$, rather than a set of tests. As soon as a test $T$ in the set $instTest(ST)$ reaches a pass verdict, the monitor stops all other tests. The test that reached a pass is allowed to conclude (by possibly giving a later fail verdict) before stopping.

The two specifications above can be realised by the use at runtime of some adequate solver for enumerating instantiations in a way similar to \cite{56} and \cite{3}. In this case, the instances are generated one at a time, until a pass event is observed; only the instances of the same symbolic test that generated the current concrete test are then considered, and no other symbolic tests are tried.

In summary, in a selection strategy for symbolic tests, we can have existential or universal selection of symbolic traces or tests, with an existential or universal selection of instances of symbolic tests. In combining the results in Section 3.2 with $UnivInstDriver(ST, SP, SUT)$ or $ExistInstDriver(ST, SP, SUT)$ presented above, what we need to do is to use these drivers as the characterisation of the execution of a symbolic test. For example, if we have an existential selection of symbolic traces (based on a property $\pi$), the set
**Existential**_trace (SUT) \_π as defined in Section 3.2 is a set of sets of symbolic tests. In this case, if universal selection of instances is required, the existential driver to be used should be as follows.

\[
\text{ExistUnivDriver}^{\text{trace}}(S, SUT) \_π = \\
\left( \left\{ \begin{array}{l}
\text{TS : Existential}_π^{\text{trace}}(S) \_π \\
\end{array} \right. \right. \\
\left\{ \begin{array}{l}
T : TS \cdot \text{UnivInstDriver}(T, SP, SUT) \}
\end{array} \right. \] \_π \cdot \\
\left\{ \begin{array}{l}
\text{TSMonitor} \\backslash \{ \{ \text{done} \} \}
\end{array} \right.
\]

This is the existential driver from Section 3.2, but the process that captures execution of a test is not \(\text{Execution}_{\text{SUT}}^S(T)\), but the universal driver \(\text{UnivInstDriver}(T, SP, SUT)\) for symbolic tests defined above. Each TS is a set of symbolic tests for the same symbolic trace. Each T in TS is, therefore, a symbolic test, which is executed by \(\text{UnivInstDriver}(T, SP, SUT)\). As soon as an instance of a symbolic test reaches a pass, just as for concrete tests, the TSMonitor stops the tests for (the instances of) symbolic tests in the other sets of symbolic tests. On the other hand, all instances of all other symbolic tests in the same set, which cover all symbolic forbidden continuations, are allowed to proceed to completion.

If, on the other hand, existential selection of instances is required, the driver to be used is as follows.

\[
\text{ExistExistDriver}^{\text{trace}}(S, SUT) \_π = \\
\left( \left\{ \begin{array}{l}
\text{TS : Existential}_π^{\text{trace}}(S) \_π \\
\end{array} \right. \right. \\
\left\{ \begin{array}{l}
T : TS \cdot \text{ExistInstDriver}(T, SP, SUT) \}
\end{array} \right. \] \_π \cdot \\
\left\{ \begin{array}{l}
\text{TSMonitor} \\backslash \{ \{ \text{done} \} \}
\end{array} \right.
\]

In this case, as soon as an instance of a symbolic test reaches a pass, the TSMonitor stops the tests for the other sets of symbolic tests. On the other hand, one instance of all other symbolic tests in the same set is allowed to complete. So, for each forbidden continuation, at least one instance is executed.

**Example 15.** For illustration, we consider \(\text{Existential}_π^{\text{trace}}(S)\) to be a set containing just two sets of symbolic tests. The first set contains tests for the symbolic trace \(\{(a, \alpha, \alpha \in \{6, 7\})\}\); we assume that the forbidden continuations for this trace are \(\{(a, \beta, \alpha \in \{6, 7\} \land \alpha = \beta\}\) and \((b, \alpha \in \{6, 7\})\). The second set of tests is for the empty trace \(\{(\), true\}\ with the single forbidden continuation \((out, \alpha, \alpha = 5)\). The first set has two tests, one for each forbidden continuation, and the second has just one symbolic test.

\[
\text{Existential}^{\text{trace}}(S) \_π = \\
\left\{ \begin{array}{l}
\text{inc} \rightarrow a : \alpha : \alpha \in \{6, 7\} \rightarrow \text{pass} \rightarrow a : \beta : \alpha \in \{6, 7\} \land \alpha = \beta \rightarrow \text{fail} \rightarrow \text{Stop}, \\
\text{inc} \rightarrow a : \alpha : \alpha \in \{6, 7\} \rightarrow \text{pass} \rightarrow b : \alpha : \alpha \in \{6, 7\} \rightarrow \text{fail} \rightarrow \text{Stop}, \\
\{\text{pass} \rightarrow \text{out} : \alpha : \alpha = 5 \rightarrow \text{fail} \rightarrow \text{Stop}\}\}
\end{array} \right.
\]

Each test in the first set has two instantiations: one where \(\alpha\) (and \(\beta\)) takes the value 6, and another where it takes the value 7. There is only one instantiation of the test in the second set. The driver for universal instantiation is the following process as defined by \(\text{ExistUnivDriver}^{\text{trace}}(S, SUT)\) at \(\pi\).

\[
\left( \left\{ \begin{array}{l}
\text{Execution}_{\text{SUT}}^S(\text{inc} \rightarrow a : 6 \rightarrow \text{pass} \rightarrow a : 6 \rightarrow \text{fail} \rightarrow \text{Stop}) \\
\text{Execution}_{\text{SUT}}^S(\text{inc} \rightarrow a : 7 \rightarrow \text{pass} \rightarrow a : 7 \rightarrow \text{fail} \rightarrow \text{Stop}) \\
\text{Execution}_{\text{SUT}}^S(\text{inc} \rightarrow a : 6 \rightarrow \text{pass} \rightarrow b \rightarrow \text{fail} \rightarrow \text{Stop}) \\
\text{Execution}_{\text{SUT}}(\text{inc} \rightarrow a : 7 \rightarrow \text{pass} \rightarrow b \rightarrow \text{fail} \rightarrow \text{Stop}) \}
\end{array} \right. \cdot \{ \{ \text{done} \} \} \\
\text{TSMonitor} \cdot \{ \{ \text{done} \} \} \\
\text{Execution}_{\text{SUT}}(\text{pass} \rightarrow \text{out} : 5 \rightarrow \text{fail} \rightarrow \text{Stop}) \cdot \{ \{ \text{done} \} \} \\
\text{TSMonitor}
\right)
\]

In this case, when one TSMonitor detects a pass event, it stops the other monitor and its tests, but lets all
its other tests run to conclusion. The driver for existential instantiation, on the other hand, is as follows.

\[
\begin{align*}
\text{Execution}_{SP}^{SUT}(\text{inc} \rightarrow \text{a.6} \rightarrow \text{pass} \rightarrow \text{a.6} \rightarrow \text{fail} \rightarrow \text{Stop}) \\
\text{Execution}_{SP}^{SUT}(\text{inc} \rightarrow \text{a.7} \rightarrow \text{pass} \rightarrow \text{a.7} \rightarrow \text{fail} \rightarrow \text{Stop})
\end{align*}
\]

\[
\begin{align*}
\text{TMonitor}
\end{align*}
\]

\[
\begin{align*}
\text{Execution}_{SP}^{SUT}(\text{inc} \rightarrow \text{a.6} \rightarrow \text{pass} \rightarrow \text{b} \rightarrow \text{fail} \rightarrow \text{Stop}) \\
\text{Execution}_{SP}^{SUT}(\text{inc} \rightarrow \text{a.7} \rightarrow \text{pass} \rightarrow \text{b} \rightarrow \text{fail} \rightarrow \text{Stop})
\end{align*}
\]

\[
\begin{align*}
\text{TMonitor}
\end{align*}
\]

\[
\begin{align*}
\text{Execution}_{SP}^{SUT}(\text{pass} \rightarrow \text{out.5} \rightarrow \text{fail} \rightarrow \text{Stop})
\end{align*}
\]

\[
\begin{align*}
\text{TMonitor}
\end{align*}
\]

In this case, once a TSMonitor detects a pass, it stops the other TSMonitor processes as before, and the TMonitor processes under its control allow one test of each set of instantiations to conclude.

For universal selection of symbolic tests, again, where Execution_{SP}^{SUT}(T) is used in the driver in Section 3.2, we can use either UnivInstDriver(T, SP, SUT) or ExistInstDriver(T, SP, SUT). Accordingly, we either have all instances or one instance of all symbolic tests run.

If the execution of one instance of one symbolic test is required, what we need is existential selection of symbolic tests, rather than symbolic traces. For the construction of the driver, we proceed as shown above.

We observe that the test drivers presented above can also handle the variant notion of instantiation with symbolic final events defining synchronisations with predicates mentioned at the end of Section 2.3.

### 3.5. Finiteness

Selection criteria must identify a finite number of tests for execution. The exhaustive test sets for a selection criteria, however, are not necessarily finite.

We have suggested the use of classical uniformity and regularity hypotheses [4]. Uniformity hypotheses are based on the definition of a finite collection of test subsets (uniformity domains), with the assumption that in each subset the tests succeed or fail uniformly. Although there is a finite number of uniformity domains, each may have an infinite number of (symbolic) tests that can contribute to coverage of that domain. In fact, uniformity hypotheses do not eliminate tests from the exhaustive test set; they just group them to form the uniformity domains since they are multiple existential selection criterion (see Section 3.2.3).

Regularity hypotheses are based on a bound of some metrics on the tests: their length, number of occurrences of some events, or number of couples of events, for instance. Typically, a regularity hypothesis eliminates tests from the exhaustive test set. In the presence of an infinite number of events, like in typical Circus specifications, regularity hypotheses may not be enough to ensure finiteness. For instance, with an infinite number of events it is possible to construct an infinite number of traces of a given size.

The need for drivers that potentially try all tests in an exhaustive test set, as explained above, can lead to drivers that do not necessarily terminate if the exhaustive test set is infinite. In the next section, we give an example of a sophisticated selection criterion for symbolic tests. We use it in Section 4.5 in the context of our framework, and show how we select finite test sets for that example.

### 4. Synchronisation coverage in Circus

So far, all our examples are based on generic properties of traces or tests for selection. In this section, we consider a more specific selection criterion, based on the coverage of synchronisations between parallel
processes of a *Circus* model. To express this criterion formally, we need to identify traces of the model that might lead to at least one such synchronisation. This is the non-trivial task that we address in this section. We identify the relevant traces of the specification from traces of its parallel components. In addition, we prove that the set that we characterise is indeed a set of traces of the specification and, therefore, adequate for use in the context of our framework to define exhaustive test sets. Our formalisation and proof is in the context of the symbolic operational semantics of *Circus*, and defines how to deal with constraints and alphabets of symbolic variables in constrained symbolic traces.

The need for specific notions of coverage for concurrent programs was recognised very early. The first precise propositions were published at the end of the eighties, when the first general concurrent programming languages appeared (see Section 5 and [55]). More specifically, synchronisation coverage was discussed in [31], where a coverage criterion based on the execution of sequences of communications is proposed, and in [5] where synchronisation coverage for Ada programs is defined and instrumented. More recent work [48, 47] has focussed on integration testing based on coverage of communications between components of distributed real-time systems specified using deterministic timed interface automata. We take inspiration from these works and consider coverage of communications (synchronisations) between parallel processes in *Circus*.

In Section 4.1, we define the set $\text{Scstrace}_{cst}^{P_1(P_1, P_2)}$ of pairs of constrained symbolic traces of parallel processes $P_1$ and $P_2$ that can lead to their synchronisation on channels in the set $cs$. We use this to define the set $\text{Scstraces}_{cst}^{cs(P_1, P_2)}$ of synchronisation traces in Section 4.2. In Section 4.3, we generalise our definitions for parallelisms involving more than two processes. Finally, in Section 4.4, we define the set $\text{select}^{P}(P)$ of synchronisation traces of any *Circus* model $P$. Our main result in this section establishes that this is a subset of the traces of $P$, as required for the selection strategies discussed in the previous section.

### 4.1. Synchronisation pairs

We consider parallel processes $P_1$ and $P_2$ and their sets of constrained symbolic traces $\text{cstraces}^{a_1}(P_1)$ and $\text{cstraces}^{a_2}(P_2)$. We identify below the sets of pairs of traces from each process that can lead to their synchronisation, at least once, when they are executed in parallel with a synchronisation set $cs$.

**Definition 12 (Synchronising constrained symbolic trace pairs).** For processes $P_1$ and $P_2$, synchronisation channel set $cs$, and disjoint alphabets $a_1$ and $a_2$, we define $\text{Scstrace}_{cst}^{P_1(P_1, P_2)}$ as follows.

$$\text{Scstrace}_{cst}^{P_1(P_1, P_2)} = \{ \text{cst}_1 : \text{cstraces}^{a_1}(P_1); \text{cst}_2 : \text{cstraces}^{a_2}(P_2) \mid \langle \text{cst}_1 \mid cs \rangle \neq \langle \rangle \land \langle \text{cst}_2 \mid cs \rangle \neq \langle \rangle \land \text{satisfiable}_{cs}(\text{cst}_1, \text{cst}_2) \}$$

A synchronising pair of traces $\text{cst}_1$ and $\text{cst}_2$ is characterised in terms of their projections to communications over channels in $cs$ and their joint satisfiability $\text{satisfiable}_{cs}(\langle \text{st}_1, c_1 \rangle, \langle \text{st}_2, c_2 \rangle)$. To avoid naming conflicts in the traces of the pair, we consider disjoint alphabets $a_1$ and $a_2$: those with no common elements.

**Example 16.** We list some of the constrained symbolic traces of the process *Components* in Section 2.1.

\[
\langle \text{in}_{a_1}, \text{left}_{\beta_1}, \alpha_1 = \beta_1 \rangle \tag{3}
\]
\[
\langle \text{in}_{a_1}, \text{left}_{\beta_1}, \text{right}_{\gamma_1}, \text{left}_{\delta_1}, \alpha_1 = \beta_1 \land \beta_1 = \delta_1 \rangle \tag{4}
\]
\[
\langle \text{in}_{a_1}, \text{left}_{\beta_1}, \text{right}_{\gamma_1}, \text{left}_{\delta_1}, \text{right}_{\epsilon_1}, \alpha_1 = \beta_1 \land \beta_1 = \delta_1 \rangle \tag{5}
\]

For the *Medium* process, some traces are as follows.

\[
\langle \text{left}_{a_2}, \text{true} \rangle \tag{6}
\]
\[
\langle \text{left}_{a_2}, \text{right}_{\beta_2}, \alpha_2 = \beta_2 \rangle \tag{7}
\]
\[
\langle \text{left}_{a_2}, \text{right}_{\beta_2}, \text{left}_{\gamma_2}, \alpha_2 = \beta_2 \rangle \tag{8}
\]
\[
\langle \text{left}_{a_2}, \text{right}_{\beta_2}, \text{left}_{\gamma_2}, 1 - \alpha_2 = \beta_2 \rangle \tag{9}
\]
\[
\langle \text{left}_{a_2}, \text{right}_{\beta_2}, \text{left}_{\gamma_2}, \text{right}_{\delta_2}, \alpha_2 = \beta_2 \land 1 - \delta_2 = \gamma_2 \rangle \tag{10}
\]
\[
\langle \text{left}_{a_2}, \text{right}_{\beta_2}, \text{left}_{\gamma_2}, \text{right}_{\delta_2}, 1 - \alpha_2 = \beta_2 \land \delta_2 = \gamma_2 \rangle \tag{11}
\]

The synchronising pairs for the parallelism between *Components* and *Medium* cannot include the empty
trace, or the traces that do not have at least one occurrence of an event representing a communication on left or right. Additionally, for example, the traces (3) and (6) above form a synchronising pair, but (3) and (7) do not, because it is not possible to match the event on right in (7): this pair of traces is not satisfiable. The traces (5) and (10), on the other hand, also form a synchronising pair.

In addition, for illustration, we consider a different action for the Receiver process in Section 2.1 used in the definition of Components. Namely, we consider right?m1 → right.m1 → . . . , instead of right?m1 → right?m2 → . . . . In this case, once the message m1 is input only another copy of m1 is accepted in the second communication via right: that is, instead of a new input right?m2, we have a synchronisation right.m1 based on m1. So, the constraint of the trace (5) above would be α1 = β1 ∧ β1 = δ1 ∧ ε1 = γ1. Such a trace would not match the trace (10), because matching requires ε1 = δ2. This is not consistent with the requirement that ε1 = γ1 because matching also requires γ1 = 1 − δ2.

In Definition 12, we require that the projections of the traces are not empty, since otherwise the pair of traces does not really lead to any synchronisation. (In fact, it is enough to require that one of them is not empty, since satisfiability requires them to be of the same length.) The projection (cst↾E cs) of a constrained symbolic trace cst to the set cs is the sequence of channels (rather than events) obtained by keeping from cst only the channels from events representing communications through a channel in cs.

Example 17. In our example, the projections of (3) and (6) to (left, right), for example, are both (left). The projection of (4) to the same set of channels is (left, right, left). Finally, the projection of (10) is (left, right, left, right).

Formal definitions for this operator and others used later are in Appendix A.

Satisfiability for pairs of (synchronising) constrained symbolic traces embeds the fact that the constraints of the traces are jointly satisfiable, even when we match the communications on the synchronisations that they require. This matching gives rise to equalities that strengthen the requirements imposed by the original individual constraints, which must be satisfiable as well.

Definition 13 (Satisfiability). For every pair (st₁, c₁) and (st₂, c₂) of constrained symbolic traces and synchronisation channel set cs, we define satisfiablecs((st₁, c₁), (st₂, c₂)) as follows.

\[ \text{satisfiable}_{cs}((\text{st}_1, c_1), (\text{st}_2, c_2)) \iff \exists a_1, a_2 \bullet (\text{st}_1 \downarrow E \ cs) =_S (\text{st}_2 \downarrow E \ cs) \land c_1 \land c_2 \]

where a₁ and a₂ are the alphabets of (st₁, c₁) and (st₂, c₂).

The equalities are defined by the operator st₄ =₅ st₄, which identifies the requirement for synchronisation of the pair of symbolic traces st₃ and st₄ containing only communications that need to synchronise. In the above definition, these traces are st₁ ↾E cs and st₂ ↾E cs. The projection st ↾E cs is similar to cst ↾E cs, but it applies to symbolic traces st and results in symbolic traces: sequences of events, rather than of channels.

Example 18. The projection of the symbolic trace (4) in Example 16 to the set (left, right), for example, is (left, β₁, right, γ₁, left, δ₁). For (10) the result of the projection is this same trace.

As formalised below, the result of st₁ =₅ st₂ is a conjunction of equalities that require that the values of the symbolic variables used to represent synchronising communications in st₁ and st₂ are the same.

Definition 14 (Conjunction of symbolic equalities). We define inductively st₁ =₅ st₂ as follows.

\[ (\langle \rangle) =_S \langle \rangle = \text{true} \]
\[ (\langle a \rangle) =_S \langle \rangle = \text{false} \]
\[ st₁ =_S \langle \rangle = \text{false} \]
\[ (⟨d₁a⟩ ∩ st₁) =_S (⟨d₁b⟩ ∩ st₂) = a = b \land (st₁ =_S st₂) \]
\[ (⟨d₁a⟩ ∩ st₁) =_S (⟨d₂b⟩ ∩ st₂) = \text{false}, \quad \text{if}\ d₁ ≠ d₂ \]

If st₁ and st₂ have different lengths or require communications over different channels, synchronisation is not possible and the requirement defined by st₁ =₅ st₂ is just false.
Example 19. For the symbolic traces of (3) and (6), we get the equality \( \beta_1 = \alpha_2 \). For (3) and (7), we get \textit{just false}. For (5) and (10), we get the conjunction of equalities \( \beta_1 = \alpha_2 \land \gamma_1 = \beta_2 \land \delta_1 = \gamma_2 \land \epsilon_1 = \delta_2 \). □

As seen in Definition 13, in \( \text{satisfiable}_{cs}(\text{st}_1, c_1), (\text{st}_2, c_2) \), the variables in the alphabets \( a_1 \) and \( a_2 \) are used in \( \langle \text{st}_1 \mid E \text{ cs} \rangle =_S \langle \text{st}_2 \mid E \text{ cs} \rangle \) and in the constraints \( c_1 \) and \( c_2 \).

4.2. Synchronisation traces

Using the notion of synchronisation pairs, we define the notion of synchronisation traces, which are constrained symbolic traces that record a parallel execution of a pair of processes (rather than separate executions of the parallel processes captured by synchronisation pairs).

Example 20. Continuing with our example, from the synchronising pair of traces (3) and (6), we get the synchronising trace \( \langle \text{in}, \alpha, \text{left}, \beta \rangle, \alpha = \beta \) over the alphabet \( \langle \alpha, \beta, \gamma, \ldots \rangle \) to capture possible observations of the parallel execution of Components and Medium. From (5) and (10), we get the synchronising trace \( \langle \text{in}, \alpha, \text{left}, \beta, \gamma, \text{left}, \delta, \text{right}, \epsilon \rangle, \alpha = \beta \land \gamma = \beta = \delta = 1 - \epsilon \). □

As defined below, synchronisation traces are characterised by the sets \( \text{Scstraces}_{cs}^{a_1, a_2}(P_1, P_2) \) of constrained symbolic traces, formed from the synchronising constrained symbolic trace pairs in \( \text{Scstraces}_{cs}^{a_1, a_2}(P_1, P_2) \), which, as formalised in Definition 12, are pairs of traces for the processes \( P_1 \) and \( P_2 \), using disjoint alphabets \( a_1 \) and \( a_2 \), and based on the synchronisation set \( cs \).

Definition 15 (Synchronising traces). For every pair of processes \( P_1 \) and \( P_2 \), synchronisation channel set \( cs \), alphabets \( a_1 \), \( a_2 \), and \( a \), we define the set \( \text{Scstraces}_{cs}^{a_1, a_2}(P_1, P_2) \) over the alphabet \( a \) as follows.

\[
\text{Scstraces}_{cs}^{a_1, a_2}(P_1, P_2) = \bigcup \{ p : \text{Scstrace}_{cs}^{a_1, a_2}(P_1, P_2) \bullet N^a \| \{ p.1[c] \ p.2 \} \}
\]

To form traces out of the pairs of traces \( p \) in \( \text{Scstrace}_{cs}^{a_1, a_2}(P_1, P_2) \), we apply the synchronisation operator \( (\text{st}_1, c_1) [ cs ] (\text{st}_2, c_2) \) (Definition 16) to the traces \( p.1 \) and \( p.2 \) in \( p \). We use \( t.i \) to refer to the \( i \)-th element of a tuple \( t \). The synchronisation operator identifies all the traces that can arise from the parallel execution of processes that can carry out the traces \( p.1 \) and \( p.2 \), synchronising on the channels in \( cs \).

Example 21. In the case of our example, from the synchronising pair of traces (3) and (6), we get the synchronising trace \( \langle \text{in}, \alpha_1, \text{left}, \beta_1 \rangle, \alpha_1 = \beta_1 \). From (5) and (10), we get a synchronising trace \( \langle \text{in}, \alpha_1, \text{left}, \alpha_2, \text{right}, \beta_2, \text{left}, \gamma, \text{left}, \delta, \text{right}, \epsilon \rangle, \alpha_1 = \alpha_2 \land \alpha_2 = \beta_2 \land \alpha_2 = \gamma_2 \land \gamma_2 = 1 - \delta_2 \). □

As illustrated above, the result of the application of \( p.1[c] \ p.2 \), as formalised in Definition 16, is a set of traces with possibly different alphabets. To obtain a set of traces over the given alphabet \( a \), we use in Definition 15 the normalising function \( N^a \) (Definition 18), which basically carries out a renaming.

Synchronisation for constrained symbolic traces is specified in Definition 16 in terms of the similar operator \( \text{st}_1[c] \text{st}_2 \) introduced in Definition 17. This new operator is for symbolic traces \( \text{st}_1 \) and \( \text{st}_2 \) and has an extra parameter: a constraint \( c \). In the specification of \( \langle \text{st}_1, c_1 \rangle [ cs ] \langle \text{st}_2, c_2 \rangle \) in Definition 16, it is applied with parameter \( c_1 \) and \( c_2 \) to capture the original constraints.

Example 22. From the synchronising pair of traces (3) and (6), the synchronisation operator for symbolic traces gives the constrained symbolic trace \( \langle \text{in}, \alpha_1, \text{left}, \beta_1 \rangle, \alpha_1 = \beta_1 \). Similarly, from (5) and (10), we get a trace with the symbolic trace \( \langle \text{in}, \alpha_1, \text{left}, \beta_1, \text{right}, \gamma, \text{left}, \delta, \text{right}, \epsilon \rangle \), and with a constraint that conjoins the original constraints of (5) and (10) and a conjunction of equalities \( \beta_1 = \alpha_2 \land \gamma_1 = \beta_2 \land \delta_1 = \gamma_2 \land \epsilon_1 = \delta_2 \) that forces the matching of their synchronised events. □

As illustrated above, synchronisation of symbolic traces gives rise to constraints that refer to variables that are not part of the resulting symbolic trace. We, therefore, in defining \( \langle \text{st}_1, c_1 \rangle [ cs ] \langle \text{st}_2, c_2 \rangle \) below, use the \( R \) function to quantify away the spurious symbolic variables, which are used in the traces of the parallel processes, but are not needed in the synchronisation trace resulting from them.
Definition 16 (Synchronisation operator - constrained symbolic traces). We define the set of synchronising constrained symbolic traces \((st_1, c_1) \parallel cs \parallel (st_2, c_2)\) as follows.

\[
(st_1, c_1) \parallel cs \parallel (st_2, c_2) = \mathcal{R}(st_1 \parallel cs \parallel (c_1 \land c_2) \parallel st_2)
\]

The synchronisation operator for symbolic traces is simply a symbolic version of the traditional traces operator in [50, p70]. It defines a set of constrained symbolic traces that can arise from synchronisation on the events involving channels in the synchronisation set \(cs\) while performing the traces \(st_1\) and \(st_2\).

Definition 17 (Synchronisation operator - symbolic traces).

\[
\begin{align*}
(st_1 \parallel cs \parallel st_2 &= st_2 \parallel cs \parallel st_1 \\
\langle \rangle \parallel cs \parallel \langle \rangle &= \{((\langle \rangle, c)\} & \text{[provided } c \text{ is satisfiable]} \\
\langle \rangle \parallel cs \parallel \langle \rangle &= \emptyset & \text{[otherwise]} \\
\langle \rangle \parallel cs \parallel \langle d, \beta \rangle &= \{((d, \beta), c)\} & \text{[provided } d \notin cs, c \text{ is satisfiable]} \\
\langle \rangle \parallel cs \parallel \langle d, \beta \rangle &= \emptyset & \text{[otherwise]} \\
((d_1, \alpha) \land st_1) \parallel cs \parallel ((d_2, \beta) \land st_2) &= \{\text{cst} : ((d_1, \alpha) \land st_1) \parallel cs \parallel st_2 \bullet ((d_2, \beta) \land \text{cst.1, cst.2})\} & \text{[provided } d_1 \in cs, d_2 \notin cs\}
\end{align*}
\]

We, first of all, establish that the synchronisation operator is commutative, and then provide an inductive definition. If both traces are empty, then we get only the empty trace itself, with constraint \(c\). A proviso guarantees that \(c\) is satisfiable, otherwise no synchronisation traces arise. If there is a conflict in the synchronisation requirements of the traces, then no synchronisation arises either. A conflict occurs when one of the traces requires synchronisation on an event on which the other is not ready to agree (either because it is empty, or its next event is a communication on a different channel also in the synchronisation set.) When there is a synchronisation on events \(d.\alpha\) and \(d.\beta\), we make an arbitrary choice to use the symbolic variable \(\beta\) in the resulting synchronisation trace. This means that \(\alpha\) is not used in that trace, but is mentioned in the constraint \(c \land \alpha = \beta\). To remove any such symbolic variables that become redundant, in Definition 16, we apply \(\mathcal{R}\) to each of the traces in \((st_1, c_1) \parallel cs \parallel (st_2, c_2)\).

As already said, the traces in \((st_1 \parallel cs \parallel st_2)\) are (potentially) over different alphabets. In the definition of \(st_{cs}(st_1, st_2)\) above, the normalisation function \(\mathcal{N}\) ensures that the constrained symbolic traces resulting from the synchronisation are over the alphabet \(a\). Alphabets keep the definition of trace equivalence simple. When defining compositions of (local) traces, however, we have the added complication of requiring normalisation. The normalisation function \(\mathcal{N}\), which is defined below, however, is just a renaming.

Definition 18 (Normalisation). For every \((st, c)\) and alphabet \(a\), we define \(\mathcal{N}^a(st, c)\) as follows.

\[
\mathcal{N}^a(st, c) = (st[a/\alpha st], c[a/\alpha st])
\]

This just changes the alphabet of \((st, c)\), whatever that is, to \(a\).
The choice of alphabets \( a_1 \) and \( a_2 \) to express the traces of the parallel processes \( P_1 \) and \( P_2 \) is irrelevant when calculating \( \text{Scstraces}^{a_1,a_2}_{cs}(P_1,P_2) \) (see Lemma 1 in Appendix C). The alphabet of the traces in this set is always \( a \). From now on, therefore, we omit these alphabets.

Our main result in this section is given by the following theorem, which establishes that every synchronising trace in \( \text{Scstraces}^{a_1,a_2}_{cs}(P_1,P_2) \) is a constrained symbolic trace of the parallelism \( P_1 \parallel \text{cs} \parallel P_2 \). In addition, they identify all traces of the parallelism that include at least one synchronisation.

**Theorem 2.**

\[
\text{Scstraces}^{a_1,a_2}_{cs}(P_1,P_2) = \{ \text{cst} : \text{cstraces}^a(P_1 \parallel \text{cs} \parallel P_2) \mid \text{cst} \upharpoonright \text{cs} \neq \langle \rangle \}
\]

This theorem establishes that if we build tests from \( \text{Scstraces}^{a_1,a_2}_{cs}(P_1,P_2) \), then we get a subset of the exhaustive test set. Its proof, and those of other theorems introduced here, can be found in Appendix D.

### 4.3. Compositionality of parallelism

So far, we have, for the sake of clarity and motivation, considered only a parallelism of two processes \( P_1 \) and \( P_2 \). It has been observed [35] that in practice the manifestation of a large majority of concurrency bugs involves no more than two threads (which correspond to parallel processes in Circus). However, we want to consider arbitrary process expressions; for instance, if we have a parallelism \( (P_1 \parallel \text{csA} \parallel P_2) \parallel \text{csB} \parallel P_3 \), then we may be interested in the synchronisations required by both \( \text{csA} \) and \( \text{csB} \). In this case, one of the parallel components is not a simple process, but a parallelism \( (P_1 \parallel \text{csA} \parallel P_2) \). A compositional approach, in which we build tests based on the (local) traces of \( P_1, P_2, \) and \( P_3 \), would be ideal.

To discuss this approach, we consider generalisations of the definitions of \( \text{Scstrace}^{a_1,a_2}_{cs}(P_1,P_2) \) and \( \text{Scstraces}^{a_1,a_2}_{cs}(P_1,P_2) \) where the sets of trace pairs or traces are built, not from processes, but from sets of traces \( \text{csts}_1 \) and \( \text{cfts}_2 \). The definitions of \( \text{Scstrace}^{a_1,a_2}_{cs}(\text{csts}_1,\text{cfts}_2) \) and \( \text{Scstraces}^{a_1,a_2}_{cs}(\text{cfts}_1,\text{cfts}_2) \) are very similar to those of \( \text{Scstrace}^{a_1,a_2}_{cs}(P_1,P_2) \) and \( \text{Scstraces}^{a_1,a_2}_{cs}(P_1,P_2) \), and are in Appendix A.

The problem that we face is that selection of synchronisation traces is actually not compositional. Precisely, if we consider \( (P_1 \parallel \text{csA} \parallel P_2) \parallel \text{csB} \parallel P_3 \) as suggested above, for instance,

\[
\text{Scstraces}^a(\text{Scstraces}^{a_1}_{cs}(\text{cstraces}^{a_1}_{cs}(P_1),\text{cstraces}^{a_2}_{cs}(P_2)),\text{cstraces}^{a_2}_{cs}(P_3)) \\
\neq \\
\text{Scstraces}^a(\text{cstraces}^{a_1}_{cs}(P_1 \parallel \text{csA} \parallel P_2),\text{cstraces}^{a_2}_{cs}(P_3))
\]

An example illustrates the issue here.

**Example 23.** The (stateless) processes that we consider are as follows.

\[
P_1 = a \rightarrow \text{Stop} \quad \Box b \rightarrow \text{Stop} \\
P_2 = a \rightarrow \text{Stop} \\
P_3 = b \rightarrow \text{Stop}
\]

We then consider the specification \( P \equiv (P_1 \parallel \{a\} \parallel P_2) \parallel \{b\} \parallel P_3 \). First of all, we consider the component \( P_1 \parallel \{a\} \parallel P_2 \), which is itself a parallelism. The traces of this parallelism are \( \langle \rangle \), \( (a) \), and \( (b) \). Its only synchronisation trace, on the other hand, is \( (a) \). If we use this synchronisation trace as a basis to construct the synchronisation traces of \( P \), we get the empty set of traces. It, however, has synchronisation trace \( (b) \), and if we want to cover both synchronisations of the specification, we actually need \( (a) \) and \( (b) \).  

This means that, in general, to construct a test set to cover all synchronisations in a model, we have to construct a test set for each of the parallelisms, considering the whole set of constrained symbolic traces of each of the components, and not only their synchronisation traces. If the synchronisation sets of the parallelisms are the same, however, we do have compositionality, as established by the following theorem.
A basic process, defined by specifying its state and action, rather than in terms of other processes, has no selectS. This is not considered in the specification of \( S \) to optimise the procedure and proceed in a compositional way.

As established by Theorem 3, in selecting traces for a parallelism, we can take advantage of nested parallelism identified by its leading to a configuration \( (c, s) \).

**Definition 19 (Terminating traces).**

\[
\text{tcstraces} \equiv \text{tcstraces}\{A | (s, c, s) \} \in \text{tcstraces} \}
\]

To cover the synchronisations in \( P \), we need to prefix its synchronisation traces with terminating traces of \( P \). We use the operator \( \text{csts} \) to form \( \text{csts} \) of \( P \). In general, different traces in \( \text{tcstraces}\{A \} \) may have different alphabets. We, therefore, use in Definition 19 the normalisation function \( N \) to obtain a set of traces over the alphabet \( a \).
Example 24. Both synchronising traces in Example 20 give rise to the synchronising trace \((\text{in}\alpha), \text{true}\) of Protocol.

Our main result here is introduced below: our selection strategy identifies a subset of the traces of a process.

Theorem 4.

\[
\text{selectS}^P(t) \subseteq \text{cstraces}^P(t)
\]

This means that selection based on \(\text{selectS}^P(t)\) identifies an unbiased test set (that is, a set of traces that can be used to construct an unbiased test set). In terms of the framework defined in the previous section, the property \(\pi(t, P)\) that can be used to achieve selection based on synchronisation coverage is \(t \in \text{selectS}^P(P)\).

We consider the use of \(\text{selectS}^P(P)\) for selection of tests for traces refinement next.

4.5. More selective synchronisation coverage

With the property \(\pi(t, SP) = t \in \text{selectS}^P(SP)\), we can define, using our framework from Section 3, two exhaustive test sets: one for existential and one for universal selection based on traces. In this example, the traces and tests are symbolic. We use the framework in Section 3, but with definitions adapted (in the expected and straightforward way) to consider symbolic traces and tests. The symbolic exhaustive test sets are shown below. In these definitions, we also rely on Theorem 4 to conclude that \(t \in \text{selectS}^P(SP)\) implies that \(t \in \text{cstraces}(SP)\) and simplify the definitions obtained directly using (1) and (2).

\[
\begin{align*}
\text{SyncExist}^P_{\text{trace}}(SP) &= \{ \text{AllTests}_T(cst, SP) \mid cst \in \text{selectS}^P(SP) \} \\
\text{SyncUniv}^P_{\text{trace}}(SP) &= \{ ST_T(cst, cse) \mid cst \in \text{selectS}^P(SP) \land cse \in \text{csinitials}(SP, cst) \}
\end{align*}
\]

Existential selection, in this example, is not very interesting, since its goal is to run only one test covering at least one synchronisation. Universal selection, on the other hand, is the basis for the property: “all tests that involve at least one synchronisation in the trace are attempted”.

The problem that we face in this section is the fact that the above sets of symbolic tests are still infinite, and, in addition, each symbolic test has an infinite number of instantiations as well. We consider next how to obtain a finite set of symbolic tests for universal selection.

For selection of symbolic tests, what we suggest is the use of a regularity hypothesis. If the model does not have unbounded nondeterminism, a regularity hypothesis that limits the size of the symbolic traces defines a finite set of symbolic tests. It is well known, however, that the choice of the limiting size must be careful, to avoid throwing away too many interesting tests [18]. In the case of synchronisation coverage, it is sensible to limit the size on the traces in such a way that ensures that all channels are used at least once.

Example 25. For synchronisation tests for the parallelism between the processes Components and Medium, the bound should be at least 8, to ensure that traces with events representing communications on out are included. For this system, we define the symbolic exhaustive set of tests (with respect to synchronisation coverage and our regularity hypothesis), as follows.

\[
\begin{align*}
\text{FSyncUniv}^P_{\text{trace}}(\text{Components} \parallel \{ \text{left}, \text{right} \} \parallel \text{Medium}) &= \\
\{ ST \mid ST \in \text{SyncUniv}^P_{\text{trace}}(\text{Components} \parallel \{ \text{left}, \text{right} \} \parallel \text{Medium}) \land \# ST \leq 9 \}
\end{align*}
\]

We use the operator \(\# ST\) to denote the size of a symbolic test: the size of its symbolic trace plus one.

For selection of instances of symbolic tests, what we suggest is the use of uniformity hypotheses based on the constraint of the symbolic traces and of the symbolic forbidden continuations. We can use the constraints to take into account information about the updates of data specified in a symbolic trace; an extreme decomposition uses a DNF characterisation of the constraints to define several domains. To be more selective, we consider each constraint as defining a single domain. In this case, selection is based on the interactions and paths of execution in the model defined by the operational semantics used to generate the symbolic traces. This means that we take the existential selection of instances of the symbolic tests (discussed in Section 3.4). This runs, if possible, one instance of every selected symbolic test.
Example 26. The driver for existential selection of instances of the tests in Example 25 is as follows.

\[
\begin{align*}
\text{SyncUnivExistDriver}^{\text{trace}}(\text{Components } & \{\text{left, right}\} & \text{Medium, SUT}) = \\
\langle \langle \langle ST : \text{FSyncUniv}^{\text{trace}}(\text{Components } & \{\text{left, right}\} & \text{Medium}) \bullet \\
\langle \langle T : \text{instTest}(ST) \bullet \text{Execution}^{SP}_{\text{SUT}}(T) \rangle \rangle & \text{inc, pass, fail } \rangle & \text{TMonitor}
\end{align*}
\]

For each of the finitely many symbolic tests in \(\text{FSyncUniv}^{\text{trace}}(\text{Components } & \{\text{left, right}\} & \text{Medium})\), we have the independent execution of its instances under the control of a TMonitor. As soon as an instance reaches a conclusive verdict, other instances are discarded.

We observe that, as illustrated in the above example, the search for a single instance may still not terminate, if none is implemented. Static choice of an instance is not a good idea, as extensively discussed in Section 3.

The exhaustivity of our test sets rely on the complete test coverage assumption to guarantee, when the SUT is nondeterministic, the execution of all its behaviours. In the case of parallel composition, it implies the spontaneous coverage of all synchronisation-race variants: this assumption can be weakened by using specific schedulers when driving the tests, such as in reachability testing [34], or CHESS [1].

5. Related works

One of the first well known coverage criteria for concurrent programs was developed by Taylor et al. [55] for Ada. It is based on notions of concurrency states and concurrency graphs used to define classical-graph coverage criteria (all-concurrency-paths, all-edges-between-cc-states, and all-cc-states), and a weaker criterion called all-possible-rendezvous, which requires that for all concurrency states that involve a rendezvous, there is at least one path through this state. This notion of coverage hides the sequential activities in the concurrency states, thus focusing on synchronisation anomalies. The authors also sketch the idea of forcing particular concurrency paths when driving test execution. As mentioned in Section 4, synchronisation coverage for Ada programs has been more precisely defined and implemented by Bron et al. [5].

Carver, Lei, Tai and others has developed reachability testing [7, 34], which provides ways to execute deterministically a concurrent program and reproduce a given test case. It is a purely dynamic method for generating synchronisation sequences (SYN-sequences) on the fly. Reachability testing algorithms are exhaustive; this ensures the execution of all the possible SYN-sequences for a given input, provided there is no unbounded loop. In this case, a bound on the length of the SYN-sequences is introduced.

For synchronous message passing, like in Circus, SYN-sequences contain pairs of sending and receiving events exercised in an execution. Deterministic execution is led according to a given SYN-sequence. Reachability testing does not address selection of test inputs or SYN-sequences, but specification-based reachability testing is addressed in [8] with a limited specification language for expressing local constraints on the SYN-sequences. When the only source of nondeterminism is race variants, reachability testing can be used to ensure the complete test assumption used in our work, since it ensures execution of all SYN-sequences.

The use of a reachability graph for structural test-sequence generation for concurrent programs is reported in [61]. A more recent approach by Souza et al. [54] reports some experiments with reachability testing and a few coverage criteria based on a notion of sync-edge association, which seems similar to the coverage of those edges corresponding to a synchronisation pair. This is close to the notion of synchronisation coverage that we proposed for Circus, but it is based on static analysis of the program.

The next generation of reachability testing algorithms is embedded in CHESS [39, 1]. This tool repeatedly runs concurrent tests ensuring that every run takes a different interleaving. If an interleaving results in an error, CHESS can reproduce it for improved debugging. The only perturbation introduced is a thin wrapper layer between the SUT and the concurrency API. The wrappers are similar to implementations of our drivers, but just like in all reachability testing techniques, they are not concerned with selection.

Dynamic test generation [6] avoids infeasible paths when generating tests from the text of a program and covering all paths. This is achieved by symbolic and standard execution in an integrated way. Test generation starts by running the program on an arbitrary concrete test input, and recording the choices and
the path followed. Afterwards, other tests are generated by switching choices to execute another path: a
constraint solver is used to check that the changes lead to feasible paths. This method has been mainly
applied to testing based on the source code of programs, as in PathCrawler [60], CUTE [53], and Dart [25].

A first difference between these approaches and our work is that our models are potentially more abstract
than the source code of programs. Secondly, similarity comes from the need to attempt alternative paths
when a test is not possible, but the main difference is that the SUT is not required to implement all the
traces of our models. Thus, our concern is absence of specification traces rather than unsatisfiability, so
we do not use constraint solving. We note that in the presence of loops, dynamic test generation may not
terminate. Termination is ensured by introducing some limit to the length of paths, which corresponds to
an implicit regularity hypothesis on the SUT. Similarly, our drivers for symbolic tests may not terminate.

Adaptive testing has been studied for the derivation of elaborate test experiments from nondeterministic
finite state machines [33] for possibly nondeterministic implementations [46, 27, 29]. The idea is to take
into account the output of the SUT to determine how to proceed with the experiment. It means that there
is no preset input sequence, but a rooted tree that anticipates all possible sequences. It is very similar
to the factorised tree-shaped tests we present in Section 3.3, which lets the SUT to lead the test. The
role of our various test drivers is a generalisation of this approach, where, in addition to the possibility of
non-implemented traces, we introduce a variety of selection strategies.

For a deterministic SUT, further work [30] has considered also the optimisation of a testing experiment
by ordering the adaptive tests. In our setting, we can consider, for example, that, if the SUT is deterministic,
an inconclusive test verdict indicates that all tests for the same trace or any of its extensions is also going
to produce an inconclusive verdict. Therefore, they are useless and can be eliminated. Sophisticated drivers
are required to order the tests and perform such optimisations.

An important feature that is missing in the semantics of Circus (and CSP) is a distinction of inputs and
outputs. The difference in the controllability of these events, with inputs controlled by the environment and
outputs by the process, is clearly important for testing. The work in [16] discusses this point in the context
of CSP and, in particular, the impact of a refinement relation that captures the distinction between inputs
and outputs on its testing theory. We note, however, that the distinction between inputs and outputs affects
the refusals of a process, but not its traces. For this reason, the results presented here for traces refinement
are not affected by considerations of controllability.

Peleska and Siegel [44, 45] applied CSP-based testing and developed a tool and technique for automation.
More recently, CSP was used by Nogueira et al. to formalise a notion of conformance traditionally associated
with input-output labelled transition systems [41], with refinement model checking used for generation and
selection of tests. This work provides a technique and a tool for generation and selection of tests based on
the use of FDR, the CSP refinement model checker. In both these works, universal selection strategies are
used, and, therefore, the issue on non-implemented traces does not arise.

In [37] Massink et al. have studied testing based on statecharts. A testing theory, in the sense of [40],
that is, for models rather than systems, as well as a notion of conformance and a test-case generation
algorithm, were presented. The theoretical framework developed follows a pattern very similar to ours, but
the considered language and the conformance relation are very different. Exhaustiveness of the generated
test set is proved, but test selection strategies are left as future work.

A symbolic version of the ioco relation [57] was stated by Frantzen et al. in [22] for Input-Output
Symbolic Transition Systems (IOSTS) implemented by input-enabled IOSTS. There is a slightly different
notion of constrained symbolic extended traces, with two constraints, one on the interaction variables, and
another on the updates of the state variables. Location coverage is mentioned as a perspective: a sort of
symbolic state coverage. This would raise the same issues we have studied and solved here, since it is an
existential coverage criterion, and ioco does not require all the traces to be implemented.

6. Conclusions

In this paper, we have identified and illustrated the problem of selection of tests for establishing traces
refinement. In short, it is not possible to have a static selection, because a correct SUT may not implement
the selected traces, in which case coverage ensured statically may not be achieved during experiments.

28
As a solution, we have proposed the use of strategies that combine the definition of an exhaustive test set with respect to the selection criteria of interest and a driver. Although, we have considered the main kinds of selection criteria, it is not ever possible to claim that we have catered for every imaginable criterion. We believe, however, that the approaches that we have proposed and illustrated for comprehensive categories of criteria can be usefully combined or extended to cater for sophisticated selection criteria. We have, in this paper, considered selection of both concrete and symbolic tests.

We have considered criteria based on one or several (multiple) properties of traces or of tests, and that require one (existential) or all (universal) implemented traces or tests that satisfy the property(ies) to be run. For each such kind of criteria, we have formalised the construction of the exhaustive test set and described a driver using Circus constructs. These driver specifications provide an accurate description of the requirements of the test experiments, but practical techniques have to consider efficient use of the SUT and of constraint solvers to avoid the use of too many copies of the SUT or instantiations of symbolic tests.

To illustrate the use of our framework, we have formalised a selection criterion for testing based on parallel Circus specifications. It is appropriate for integration testing, and requires coverage of synchronisations between parallel processes in a specification. We have formally defined this trace selection criterion and, specified an algorithm for selection. We have proved that this algorithm generates traces of the specification, and, therefore, unbiased tests. This is used to define a finite set of symbolic tests and accompanying driver.

The problem raised by the possibility of selecting non-implemented traces is also raised by a different conformance relation that we have studied previously in the context of Circus, namely, conf. What conf requires is that, for traces that are common to the specification and the SUT, the SUT deadlocks only when a deadlock is allowed in the model. As opposed to the tests for traces refinement, tests for conf are positive. They check that, after a given trace of the specification, at least one event from a set of minimal acceptances is accepted by the SUT. Since conf is restricted to traces that are common to the SUT and the specification, if the trace is not implemented by the SUT, we again have an inconclusive verdict. We show in [14] that the same solutions proposed here are applicable in testing for conf.

This is an important result because we have previously shown that failures refinement, another important conformance relation for both CSP and Circus, can be characterised as the conjunction of traces refinement and conf [10, 13]. An exhaustive test set for failures refinement is, therefore, the union of the exhaustive test sets for traces refinement and for conf. Moreover, while traces refinement is concerned with safety properties and cannot, for instance, detect a mismatch in the alphabet of events of an SUT, conf can be used to identify such a problem. If the SUT insists in performing an event outside of the alphabet of the specification, unless a deadlock is allowed by the specification, a test for conf can identify the problem.

A popular conformance relation is ioco [57]. Since it allows that some traces of the specification not to be implemented, our results are of interest for test selection in the case of ioco.

As for future work we are interested in performing case studies, both in the form of the definition of additional selection criteria and experiments of testing actual systems. In that respect, the automation of the Circus testing theory presented in [19, 20] is of great relevance.

Also of interest is the application of the ideas presented here to the notion of traces for Circus defined in [12] and [15]. In that work, we consider traces that record information about the data operations (specification statements, assignments, guards, and so on) in the Circus specification, and support selection techniques based on the structure of the model: in [15] we present several data flow coverage criteria for Circus specifications. Just like the symbolic traces of the original Circus testing theory, these symbolic traces do not need to be implemented by an SUT. So, the same issues raised here apply.

Acknowledgements. We are grateful to the Royal Society and the CNRS for funding our collaboration via their International Exchange scheme, and to Rob Hierons for various discussions. We are also indebted to anonymous referees for their careful revision and useful suggestions.

References

REFERENCES


References


Appendix A. Formal definitions of operators

Definition 21. We define a pair of alphabets \( a_1 \) and \( a_2 \) to be disjoint if their sets of elements are disjoint: \( \text{disjoint}(a_1, a_2) = \text{ran} a_1 \cap \text{ran} a_2 = \emptyset \).

Definition 22. For every constrained symbolic trace \((st, c)\) and synchronisation channel set \(cs\), we define the projection \((st, c) \mid_c cs\) of the trace \((st, c)\) to channels in \(cs\) as \((st, c) \mid_c cs = st \mid_c cs\), where the similar projection operator for symbolic traces is defined inductively as follows.

\[
\begin{align*}
\langle \rangle \mid_c cs & = \langle \rangle \\
((d, a) \triangleright st) \mid_c cs & = (d) \triangleright (st \mid_c cs), \text{ if } d \in cs \\
((d, a) \triangleright st) \mid_c cs & = st \mid_c cs, \text{ if } d \notin cs
\end{align*}
\]

Definition 23. For every symbolic trace \(st\) and synchronisation channel set \(cs\), we define inductively the projection \(st \mid_E cs\) of \(st\) to events representing communications over channels in \(cs\) as follows.

\[
\begin{align*}
\langle \rangle \mid_E cs & = \langle \rangle \\
((d, a) \triangleright st) \mid_E cs & = (d) \triangleright (st \mid_E cs), \text{ if } d \in cs \\
((d, a) \triangleright st) \mid_E cs & = st \mid_E cs, \text{ if } d \notin cs
\end{align*}
\]

Definition 24. For sets of constrained symbolic traces \(csts_1\) and \(csts_2\) with disjoint alphabets, and channel set \(cs\), we define the set of synchronising pairs \(\text{ScstraceP}_c(csts_1, csts_2)\) as follows.

\[
\text{ScstraceP}_c(csts_1, csts_2) = \{cst_1 : csts_1; \ cst_2 : csts_2 \mid (cst_1 \mid_c cs) \neq \langle \rangle \land (cst_2 \mid_c cs) \neq \langle \rangle \land \text{satisfiable}_c(cst_1, cst_2)\}
\]

Definition 25. For sets of constrained symbolic traces \(csts_1\) and \(csts_2\), channel set \(cs\), and alphabet \(a\) we define the set \(\text{Scstraces}_c^a(csts_1, csts_2)\) of synchronising constrained symbolic traces over \(a\) as follows.

\[
\text{Scstraces}_c^a(csts_1, csts_2) = \bigcup\{p : \text{ScstraceP}_c(csts_1, csts_2) \bullet N^a \langle p1 \mid cs \mid p2 \rangle\}
\]

Definition 26.

\[
csts_1 \text{ ccat } csts_2 = \{st_1, st_2, c_1, c_2 \mid (st_1, c_1) \in csts_1 \land (st_2, c_2) \in csts_2 \bullet (st_1 \triangleright st_2, c_1 \land c_2)\}
\]

Definition 27. For every constrained symbolic trace \((st, c)\) and synchronisation channel set \(cs\), we define the projection \((st, c) \mid_c cs\) of the trace \((st, c)\) to channels not in \(cs\) as \((st, c) \mid_c cs = R(st \mid_c cs, c)\), where the projection operator for symbolic traces is defined inductively as follows.

\]

\[
\begin{align*}
\langle \rangle \mid_c cs & = \langle \rangle \\
((d, a) \triangleright st) \mid_c cs & = (d) \triangleright (st \mid_c cs), \text{ if } d \notin cs \\
((d, a) \triangleright st) \mid_c cs & = st \mid_c cs, \text{ if } d \in cs
\end{align*}
\]

Appendix B. Properties of the Circus operational semantics

The following propositions establish basic properties of the Circus operational semantics that we need. A simple property is captured by the proposition below. It states that, if the action does not involve a variable \(x\), or more generally, any of the variables in a state \(s_3\), then its value in the state is not changed.

Proposition 1.

\[
(c_1 \mid s_1 = A_1) \xrightarrow{st} (c_2 \mid s_2 = A_2)
\]

if, and only if,

\[
(c_1 \mid s_1; s_3 = A_1) \xrightarrow{st} (c_2 \mid s_2; s_3 = A_2)
\]

provided \(\text{FV}(s_3) \cap \text{FV}(A_1) = \emptyset\).

\(\text{FV}(A)\) is the set of free variables of the action \(A\) as defined in [42]. In addition, if a constraint \(c_3\) is over
symbolic variables that are not used in the state nor in the symbolic trace, then it can be ignored.

**Proposition 2.**

\[(c_1 \mid s_1 \models A_1) \xrightarrow{st} (c_2 \mid s_2 \models A_2)\]

if, and only if,

\[(c_1 \land c_3 \mid s_1 \models A_1) \xrightarrow{st} (c_2 \land c_3 \mid s_2 \models A_2)\]

provided \(FV(c_3) \cap SV(s_1, s_2) = \emptyset\) and \(FV(c_3) \cap \alpha st = \emptyset\).

We use \(SV(s)\) to denote the set of symbolic variables used in the definition of \(s\) (or, more generally, in a list of states \(s_1, s_2\) as used in the proposition above). By construction, constraints of a configuration are only ever strengthened.

**Proposition 3.**

\[(c_1 \mid s_1 \models A_1) \xrightarrow{st} (c_2 \mid s_2 \models A_2)\]

if, and only if, for some \(c_3\)

\[(c_1 \mid s_1 \models A_1) \xrightarrow{st} (c_1 \land c_3 \mid s_2 \models A_2)\]

So, the constraint \(c_1\) used in an initial configuration is preserved in any configuration reached from it.

The operational semantics is consistent with the denotational semantics. So, for example, we have the property below for traces of an external choice.

**Proposition 4.**

\[(c_1 \mid s_1 \models A_1 \boxdot A_2) \xrightarrow{st} (c_2 \mid s_2 \models A_3)\]

for some \(s_2\) and \(A_3\) if, and only if,

\[(c_1 \mid s_1 \models A_1) \xrightarrow{st} (c_2 \mid s_2 \models A_3)\]

or \(c_1 \mid s_1 \models A_2\) \xrightarrow{st} \(c_2 \mid s_2 \models A_3\).

This is consistent with the denotational semantics of \(A_1 \boxdot A_2\), which defines that its set of traces is the union of those of \(A_1\) and \(A_2\). For sequential composition, we have the following.

**Proposition 5.**

\[(c_1 \mid s_1 \models A_1 \cdot A_2) \xrightarrow{st} (c_2 \mid s_2 \models A_3)\]

for some \(s_2\) and \(A_3\) if, and only if,

\[(c_1 \mid s_1 \models A_1) \xrightarrow{st} (c_2 \mid s_2 \models A_3)\]

or, there are \(st_1, c'_1, s'_1\), and \(st_2\) such that \(st = st_1 \land st_2\),

\[(c_1 \mid s_1 \models A_1) \xrightarrow{st} (c'_1 \mid s'_1 \models \text{Skip})\]

and \((c'_1 \mid s'_1 \models A_2) \xrightarrow{st_2} (c_2 \mid s_2 \models A_3)\).

The next property is concerned with the semantics of parallel actions. It relates the traces of a parallelism \(A_1 \parallel c s \parallel A_2\) of actions, as calculated by the operational semantics, with the result of applying the synchronisation operator to the traces \(st_1\) and \(st_2\) of the parallel actions \(A_1\) and \(A_2\). This is needed in this work, where we consider parallel processes, because parallelism of processes is defined in terms of the parallelism of their main actions, with name sets defined by the states of the processes.
Proposition 6.

\[(c_1 | s_1 \models A \upharpoonright | x_1 | cs | x_2 \upharpoonright A_2) \xrightarrow{st} (c_2 | s_2 \models A_3)\]

for some \(s_2\) and \(A_3\) if, and only if, there are \(st_1, c_1', s_1', A_1', st_2, c_2', s_2', A_2',\) and \(a\), such that \(\alpha c_1' \cap \alpha c_2' = \emptyset\), \(\alpha st_1 \subseteq \alpha c_1',\) \(\alpha st_2 \subseteq \alpha c_2',\) \(\alpha st \leq a\).

\[(c_1 | s_1 \models A_1) \xrightarrow{st} (c_1' | s_1' \models A_1')\]

and

\[\mathcal{R}(st, c_2) \in \mathcal{N}^a \{ \mathcal{R} \upharpoonright \langle st_1 \upharpoonright [cs \upharpoonright (c_1' \land c_2') \upharpoonright st_2] \rangle \}\]

We need to apply \(\mathcal{R}\) to all constrained symbolic traces: that obtained from the operational semantics of \(A_1 \upharpoonright x_1 \upharpoonright cs \upharpoonright x_2 \upharpoonright A_2\) and those obtained by the synchronisation of \(st_1\) and \(st_2\). The renaming carried out by \(\mathcal{N}^a\) ensures that all symbolic traces are over the same alphabet \(a\), and so, can be compared.

Finally, we have a property of the operational semantics of hiding.

Proposition 7.

\[(c_1 | s_1 \models A \upharpoonright \text{cs}) \xrightarrow{st} (c_2 | s_2 \models A_2)\]

for some \(s_2\) and \(A_3\) if, and only if, there are \(st_2, c_3, s_3, A_3,\) and \(a\), such that \(\alpha st_1 \leq a\),

\[(c_1 | s_1 \models A) \xrightarrow{st} (c_3 | s_3 \models A_3)\quad \text{and} \quad \mathcal{R}(st_1, c_2) = \mathcal{N}^a(\mathcal{R}(st_2, c_3) \upharpoonright | c \text{cs})\]

We consider traces \(st_2\) defined by the evaluation of \(A\), and their projections to remove the channels in \(cs\).

Appendix C. Some lemmas and their proofs

Lemma 1.

\[Scstraces^{a_1, a_2}_{cs}(P_1, P_2) = Scstraces^{a_1, a_2}_{cs}(P_1, P_2)\]

Proof. There is a bijection between \(cstraces^{a_1}(P_1)\) and \(cstraces^{a_2}(P_1)\) reflecting the fact that their symbolic traces characterise the same set of traces, namely those of \(P_1\), and the only difference between the symbolic traces in these sets is in their use of names of symbolic variables. The same comment applies to \(cstraces^{a_1}(P_2)\) and \(cstraces^{a_2}(P_2)\). We, therefore, can conclude that there is such a bijection between \(Scstraces^{a_1, a_2}_{cs}(P_1, P_2)\) and \(Scstraces^{a_1, a_2}_{cs}(P_1, P_2)\). So, this lemma is a direct consequence of the definition of \(\mathcal{N}^a\). \(\square\)

Appendix C.1. Properties of synchronisation

The constraints of all traces are the same.

Lemma 2.

\[\forall \text{cs} : st_1 \upharpoonright cs \upharpoonright cs \cdot st_2 = (st_1 \upharpoonright E \text{cs} = s \upharpoonright st_2 \upharpoonright E \text{cs} )\land \text{c}\]

Proof. By induction.

Case 1.

\[(st, c_1) \in \langle \rangle \upharpoonright \langle cs, c_2 \rangle \langle \rangle\]

\[\Rightarrow c_1 = c_2\]

[definition of \((\langle \rangle \upharpoonright cs, c_2 \upharpoonright \langle \rangle)\)]

\[\Leftrightarrow c_1 = (\langle \langle \rangle \upharpoonright E \text{cs} \rangle = s (\langle \langle \rangle \upharpoonright E \text{cs} )) \land c_2\]

[definition of \(\upharpoonright E\) and \(= s\)]
Case 2.

\[(\text{st}, c_1) \in (\langle \text{cs}, c_2 \rangle \parallel (\text{d}, \beta)) \]
\[\Rightarrow c_1 = c_2 \quad \text{[definition of } \langle \text{cs}, c_2 \rangle \parallel (\text{d}, \beta)]\]
\[\Leftrightarrow c_1 = ((\langle \text{cs} \parallel \text{c} \rangle =_5 (\langle \text{d}, \beta \rangle \parallel \text{cs})) \land c_2 \quad \text{[}(\langle \text{d}, \beta \rangle \parallel \text{cs}) = \langle \rangle]\]

Case 3.

\[(\text{d}_1 \in \text{cs}, \text{d}_2 \notin \text{cs})\]
\[(\text{st}, c_1) \in ((\langle \text{d}_1, \alpha \rangle \parallel \text{st}_1) \parallel \text{cs}, c_2) \parallel (\langle \text{d}_2, \beta \rangle \parallel \text{st}_2)\]
\[\Rightarrow \exists \text{st}_3, c_3 \in ((\langle \text{d}_1, \alpha \rangle \parallel \text{st}_1) \parallel \text{cs}, c_2 \parallel \text{st}_2) \land \text{st}_1 = (\langle \text{d}_2, \beta \rangle \parallel \text{st}_3) \land c_1 = c_3 \]
\[\quad \text{[definition of } (\langle \text{d}_1, \alpha \rangle \parallel \text{st}_1) \parallel \text{cs}, c_2 \parallel (\langle \text{d}_2, \beta \rangle \parallel \text{st}_2)]\]
\[\Leftrightarrow \exists \text{st}_3, c_3 \in ((\langle \text{d}_1, \alpha \rangle \parallel \text{st}_1) \parallel \text{cs}, c_2 \parallel \text{st}_2) \land \text{st}_1 = (\langle \text{d}_2, \beta \rangle \parallel \text{st}_3) \land c_1 = c_3 \]
\[\quad \text{[predicate calculus]}\]
\[\Rightarrow c_1 = ((\langle \text{d}_1, \alpha \rangle \parallel \text{st}_1) \parallel \text{cs} =_5 \text{st}_2 \parallel \text{cs}) \land c_2 \]
\[\quad \text{[induction hypothesis]}\]
\[\Leftrightarrow c_1 = ((\langle \text{d}_1, \alpha \rangle \parallel \text{st}_1) \parallel \text{cs} =_5 (\langle \text{d}_2, \beta \rangle \parallel \text{st}_2) \parallel \text{cs}) \land c_2 \]
\[\quad \text{[}(\langle \text{d}_2, \beta \rangle \parallel \text{st}_2) \parallel \text{cs} = \text{st}_2 \parallel \text{cs}]\]

Case 4.

\[(\text{d} \in \text{cs})\]
\[(\text{st}, c_1) \in ((\langle \text{d}, \alpha \rangle \parallel \text{st}_1) \parallel \text{cs}, c_2) \parallel (\langle \text{d}, \beta \rangle \parallel \text{st}_2)\]
\[\Leftrightarrow \exists \text{st}_3, c_3 \in \text{st} \parallel (\text{cs}, (c_2 \land \alpha = \beta)) \parallel \text{st}_2 \land \text{st}_1 = (\langle \text{d}, \beta \rangle \parallel \text{st}_3) \]
\[\quad \text{[definition of } (\langle \text{d}, \alpha \rangle \parallel \text{st}_1) \parallel \text{cs}, c_2 \parallel (\langle \text{d}, \beta \rangle \parallel \text{st}_2)]\]
\[\Rightarrow c_1 = ((\langle \text{d}, \alpha \rangle \parallel \text{st}_1) \parallel \text{cs} = _5 \text{st}_2 \parallel \text{cs}) \land (c_2 \land \alpha = \beta) \]
\[\quad \text{[induction hypothesis]}\]
\[\Leftrightarrow c_1 = ((\langle \text{d}, \alpha \rangle \parallel \text{st}_1) \parallel \text{cs} = _5 (\langle \text{d}, \beta \rangle \parallel \text{st}_2) \parallel \text{cs}) \land c_2 \]
\[\quad \text{[definition of } =_5]\]
\[\Rightarrow c_1 = ((\langle \text{d}, \alpha \rangle \parallel \text{st}_1) \parallel \text{cs} = _5 (\langle \text{d}, \beta \rangle \parallel \text{st}_2) \parallel \text{cs}) \land c_2 \]
\[\quad \text{[}(\langle \text{d}, \alpha \rangle \parallel \text{st}_1) \parallel \text{cs} = \langle \text{d}, \alpha \rangle \parallel (\text{st}_1 \parallel \text{cs}) \text{ and } (\langle \text{d}, \beta \rangle \parallel \text{st}_2) \parallel \text{cs} = \langle \text{d}, \beta \rangle \parallel (\text{st}_2 \parallel \text{cs})]\]

Case 5.

\[(\text{d}_1 \notin \text{cs}, \text{d}_2 \notin \text{cs})\]
\[(\text{st}, c_1) \in (((\langle \text{d}_1, \alpha \rangle \parallel \text{st}_1) \parallel \text{cs}, c_2) \parallel (\langle \text{d}_2, \beta \rangle \parallel \text{st}_2))\]
\[\Rightarrow \exists \text{st}_3, c_3 \in (((\langle \text{d}_1, \alpha \rangle \parallel \text{st}_1) \parallel \text{cs}, c_2) \parallel \text{st}_2) \lor\]
\[\quad (\text{st}_3, c_1) \in (\text{st}_1 \parallel (\text{cs}, c_2) \parallel (\langle \text{d}_2, \beta \rangle \parallel \text{st}_2))\]
\[\quad \text{[definition of } (\langle \text{d}_1, \alpha \rangle \parallel \text{st}_1) \parallel \text{cs}, c_2 \parallel (\langle \text{d}_2, \beta \rangle \parallel \text{st}_2)]\]
\[\Rightarrow c_1 = (((\langle \text{d}_1, \alpha \rangle \parallel \text{st}_1) \parallel \text{cs} =_5 \text{st}_2 \parallel \text{cs}) \land c_2 \lor\]
\[\quad \text{[induction hypothesis]}\]
\[\quad c_1 = (\text{st}_1 \parallel \text{cs} =_5 (\langle \text{d}_2, \beta \rangle \parallel \text{st}_2) \parallel \text{cs}) \land c_2\]
\[\Rightarrow c_1 = (((\langle \text{d}_1, \alpha \rangle \parallel \text{st}_1) \parallel \text{cs} =_5 (\langle \text{d}_2, \beta \rangle \parallel \text{st}_2) \parallel \text{cs}) \land c_2\]
\[\quad \text{[}(\langle \text{d}_1, \alpha \rangle \parallel \text{st}_1) \parallel \text{cs} = (\text{st}_1 \parallel \text{cs}) \text{ and } (\langle \text{d}_2, \beta \rangle \parallel \text{st}_2) \parallel \text{cs} = (\text{st}_2 \parallel \text{cs})]\]

\[\square\]

The projection of the synchronisation traces in \(\text{st}_1 \parallel \text{cs}, \text{c} \parallel \text{st}_2\) to their symbolic traces does not change if we quantify one of the variables (potentially) free in \(c\).

Lemma 3.

\[(\text{st}_1 \parallel \text{cs}, \text{c} \parallel \text{st}_2).1 = (\text{st}_1 \parallel \text{cs}, (\exists x \bullet \text{c}) \parallel \text{st}_2).1\]
Proof. By induction.

Case 1(a). : provided \( c \)

\[
\langle l \rangle \ [\text{cs}, c \] \langle r \rangle \} .1
\]

\[
= \langle l \rangle \ [\text{cs}, c \] \langle r \rangle \} .1
\]

\[
= \{ r \}
\]

\[
= \langle l \rangle \ [\text{cs}, (\exists x \bullet c) \} \} .1
\]

\[
= \langle l \rangle \ [\text{cs}, (\exists x \bullet c) \} \langle r \rangle \} .1
\]

[synchronisation operator]

[relational image]

[relational image]

[synchronisation operator]

Case 1(b). : otherwise

\[
\langle l \rangle \ [\text{cs}, c \] \langle r \rangle \} .1
\]

\[
= \emptyset
\]

[synchronisation operator and relational image]

[(\exists x \bullet c) does not hold]

Case 2(a). : (\langle l \rangle \ [cs, c \ [\langle r \rangle \}) , provided \( c \)

\[
\langle l \rangle \ [cs, c \ [\langle r \rangle \}) .1
\]

\[
= \langle l \rangle \ [cs, c \ [\langle r \rangle \}) .1
\]

\[
= \{ r \}
\]

[relational image]

[relational image]

[relational image]

[synchronisation operator]

Case 2(a). : (\langle l \rangle \ [cs, c \ [\langle r \rangle \}) , provided \( c \) does not hold

Similar to Case 1(b).

Case 3.: \( d_1 \in \text{cs}, d_2 \notin \text{cs} \)

\[
\langle (d_1, \alpha) \ 
\]

\[
\langle l \rangle \ [cs, c \ [\langle r \rangle \}) .1
\]

\[
= \langle l \rangle \ [cs, c \ [\langle r \rangle \}) .1
\]

\[
= \{ r \}
\]

[relational image]

[relational image]

[relational image]

[synchronisation operator]

Case 4.: \( d \in \text{cs} \)

\[
\langle (d, \alpha) \ 
\]

\[
\langle l \rangle \ [cs, c \ [\langle r \rangle \}) .1
\]

\[
= \langle l \rangle \ [cs, c \ [\langle r \rangle \}) .1
\]

\[
= \{ r \}
\]

[relational image]

[relational image]

[synchronisation operator]

36
Case 6.: \( (d_1, \alpha) \land \text{st}_1 \) \( [cs, c] (d_2, \beta) \land \text{st}_2 \), with \( d_1 \neq d_2, d_1 \in cs, d_2 \in cs \)
Similar to Case 1(b).

\[
\{(d_1, \alpha) \land \text{st}_1 \} [cs, c] \{(d_2, \beta) \land \text{st}_2 \} \]

\[
\text{[synchronisation operator]}
\]

\[
\{(d_1, \alpha) \land \text{st}_1 \} [cs, c] \text{st}_2 \bullet \{(d_2, \beta) \land \text{st}_1 \} \bullet \{(d_1, \alpha) \land \text{st}_2 \} \}
\]

\[
\text{[property of relational image]}
\]

\[
\{(d_1, \alpha) \land \text{st}_1 \} [cs, \exists x \cdot c] \text{st}_2 \bullet \{(d_2, \beta) \land \text{st}_1 \} \bullet \{(d_1, \alpha) \land \text{st}_2 \} \}
\]

\[
\text{[induction hypothesis]}
\]

\[
\{(d_1, \alpha) \land \text{st}_1 \} [cs, \exists x \cdot c] \{(d_2, \beta) \land \text{st}_1 \} \bullet \{(d_1, \alpha) \land \text{st}_2 \} \}
\]

\[
\text{[property of relational image]}
\]

\[
\{(d_1, \alpha) \land \text{st}_1 \} [cs, \exists x \cdot c] \{(d_2, \beta) \land \text{st}_2 \} \}
\]

\[
\text{[synchronisation operator]}
\]

In the lemma below, we have a simple property of \( R \) when used in conjunction with the synchronisation operator. Basically, we can, in advance, consider a weaker constraint that already quantifies away variables that represent internal values: those that are not used in either of the traces \( \text{st}_1 \) and \( \text{st}_2 \) synchronised.

**Lemma 4.**

\[
R \{ \text{st}_1 [cs, c] \text{st}_2 \} = R \{ \text{st}_1 [cs, (\exists \alpha \cdot \alpha(\text{st}_1, \text{st}_2) \bullet c]) \text{st}_2 \}
\]

**Proof.**

\[
R \{ \text{st}_1 [cs, c] \text{st}_2 \}
\]

\[
\text{[relational image]}
\]

\[
\text{[Lemma 2]}
\]

\[
\text{[definition of R, with x_1 = \alpha(\text{st}_1 [E cs, st_2 |E cs, c]) \cdot \alpha cst.1]}
\]

\[
\text{[property of sets, with x_2 = (\alpha(\text{st}_1 [E cs, st_2 |E cs, c]) \cdot \alpha cst.1]}
\]

\[
\text{[property of sets, with x_3 = (\alpha(\text{st}_1 [E cs, st_2 |E cs, c]) \cdot \alpha cst.1]}
\]

\[
\text{[predicate calculus, with x_4 = (\alpha(\text{st}_1 [E cs, st_2 |E cs, c]) \cdot \alpha cst.1]}
\]

37
The following lemma establishes that the set of traces \( \text{st}_1 \sqcap \{ \text{cs} \mid (\exists \alpha (\alpha \sqcap \alpha (\text{st}_1, \text{st}_2)) \} \sqcap \text{st}_2 \) is not empty exactly when \( \alpha \) is satisfiable, even in the presence of the synchronisation requirements imposed by \( \text{st}_1 \) and \( \text{st}_2 \).

**Lemma 5.**

\[
(\text{st}_1 \sqcap \text{cs} \sqcap \text{st}_2) \neq \emptyset \iff \exists \alpha_1, \alpha_2 \cdot (\text{st}_1 \sqcap \text{cs} \sqcap \text{st}_2) = (\text{st}_1 \sqcap \text{cs} \sqcap \text{st}_2) \land \alpha
\]

where \( \alpha \text{st}_1 \leq \alpha_1 \) and \( \alpha \text{st}_2 \leq \alpha_2 \).

**Proof.** By induction.

**Case 1.**

\[
(\langle \rangle \sqcap \text{cs} \sqcap \langle \rangle) \neq \emptyset \\
\iff c \\
\iff \exists \alpha_1, \alpha_2 \cdot (\langle \rangle \sqcap \text{cs} \sqcap \langle \rangle) = (\langle \rangle \sqcap \text{cs} \sqcap \langle \rangle) \land \alpha
\]

where \( \langle \rangle \) and \( \langle \rangle = (\langle \rangle \sqcap \text{cs} \sqcap \langle \rangle) = \text{true} \)

**Case 2(a).** \( : d \notin \text{cs} \)

\[
(\langle \rangle \sqcap \text{cs} \sqcap \langle d, \beta \rangle) \neq \emptyset \\
\iff c \\
\iff \exists \alpha_1, \alpha_2 \cdot (\langle \rangle \sqcap \text{cs} \sqcap \langle d, \beta \rangle) = (\langle \rangle \sqcap \text{cs} \sqcap \langle d, \beta \rangle) \land \alpha
\]

where \( (\langle \rangle \sqcap \text{cs} \sqcap \langle d, \beta \rangle) = (\langle \rangle \sqcap \text{cs} \sqcap \langle d, \beta \rangle) = \text{false} \)

**Case 2(b).** \( : d \in \text{cs} \)

\[
(\langle \rangle \sqcap \text{cs} \sqcap \langle d, \beta \rangle) \neq \emptyset \\
\iff \exists \alpha_1, \alpha_2 \cdot (\langle \rangle \sqcap \text{cs} \sqcap \langle d, \beta \rangle) = (\langle \rangle \sqcap \text{cs} \sqcap \langle d, \beta \rangle) \land \alpha
\]

where \( (\langle \rangle \sqcap \text{cs} \sqcap \langle d, \beta \rangle) = (\langle \rangle \sqcap \text{cs} \sqcap \langle d, \beta \rangle) = \text{false} \)

**Case 3.** \( : d_1 \in \text{cs}, d_2 \notin \text{cs} \)

\[
((\langle d_1, \alpha \rangle \sqcap \text{st}_1) \sqcap \text{cs} \sqcap ((\langle d_2, \beta \rangle \sqcap \text{st}_2)) \neq \emptyset \\
\iff ((\langle d_1, \alpha \rangle \sqcap \text{st}_1) \sqcap \text{cs} \sqcap ((\langle d_2, \beta \rangle \sqcap \text{st}_2)) \neq \emptyset \\
\iff \exists \alpha_1, \alpha_2 \cdot ((\langle d_1, \alpha \rangle \sqcap \text{st}_1) \sqcap \text{cs} \sqcap ((\langle d_2, \beta \rangle \sqcap \text{st}_2)) \land \alpha
\]

where \( ((\langle d_1, \alpha \rangle \sqcap \text{st}_1) \sqcap \text{cs} \sqcap ((\langle d_2, \beta \rangle \sqcap \text{st}_2)) = (\text{st}_2 \sqcap \text{cs}) \land \alpha \)

**Case 4.** \( : d \in \text{cs} \)

\[
((\langle d, \alpha \rangle \sqcap \text{st}_1) \sqcap \text{cs} \sqcap ((\langle d, \beta \rangle \sqcap \text{st}_2)) \neq \emptyset \\
\iff (\langle d, \alpha \rangle \sqcap \text{st}_1) \sqcap \text{cs} \sqcap ((\langle d, \beta \rangle \sqcap \text{st}_2)) \neq \emptyset \\
\iff \exists \alpha_1, \alpha_2 \cdot ((\langle d, \alpha \rangle \sqcap \text{st}_1) \sqcap \text{cs} \sqcap ((\langle d, \beta \rangle \sqcap \text{st}_2)) \land \alpha
\]

where \( ((\langle d, \alpha \rangle \sqcap \text{st}_1) \sqcap \text{cs} \sqcap ((\langle d, \beta \rangle \sqcap \text{st}_2)) = (\text{st}_2 \sqcap \text{cs}) \land \alpha \)

\[
38
\]
Case 5.: \( d_1 \neq d_2, d_1 \in \text{cs}, d_2 \in \text{cs} \)

\[((d_1, \alpha) \land \text{st}_1) \| \text{cs}, c \| ((d_2, \beta) \land \text{st}_2) \rangle \neq \emptyset \)

\( \iff \) \( \color{red}{\text{false}} \) [definition of \( ((d_1, \alpha) \land \text{st}_1) \| \text{cs}, c \| ((d_2, \beta) \land \text{st}_2) \rangle \)]

\( \implies \exists a_1, a_2 \cdot \left( ((d_1, \alpha) \land \text{st}_1) \| \text{E} \text{cs} = \emptyset \right) \iff \left( ((d_2, \beta) \land \text{st}_2) \| \text{E} \text{cs} \right) \land \text{c} \)

\( \left( ((d_1, \alpha) \land \text{st}_1) \| \text{E} \text{cs} \right) = \emptyset \iff \left( ((d_2, \beta) \land \text{st}_2) \| \text{E} \text{cs} \right) \land \text{c} \)

\( [\text{induction hypothesis}] \)

Case 6.: \( d_1 \not\in \text{cs}, d_2 \not\in \text{cs} \)

\( \left( ((d_1, \alpha) \land \text{st}_1) \| \text{cs}, c \| ((d_2, \beta) \land \text{st}_2) \rangle \neq \emptyset \)

\( \iff \left( ((d_1, \alpha) \land \text{st}_1) \| \text{cs}, c \| \text{st}_2 \rangle \neq \emptyset \lor \left( \text{st}_1 \| \text{cs}, c \| ((d_2, \beta) \land \text{st}_2) \rangle \neq \emptyset \right) \)

\( [\text{definition of } ((d_1, \alpha) \land \text{st}_1) \| \text{cs}, c \| ((d_2, \beta) \land \text{st}_2) \rangle ] \]

\( \iff \left( \exists a_1, a_2 \cdot \left( ((d_1, \alpha) \land \text{st}_1) \| \text{E} \text{cs} = \emptyset \right) \iff \left( ((d_2, \beta) \land \text{st}_2) \| \text{E} \text{cs} \right) \land \text{c} \)

\( \left( \exists a_1, a_2 \cdot \left( ((d_1, \alpha) \land \text{st}_1) \| \text{E} \text{cs} = \emptyset \right) \iff \left( ((d_2, \beta) \land \text{st}_2) \| \text{E} \text{cs} \right) \land \text{c} \)

\( [\text{induction hypothesis}] \)

With the next lemma, we establish that, if the projection of both traces \( \text{st}_1 \) and \( \text{st}_2 \) to synchronisation channels is nonempty, then the projection of all synchronisation traces to these channels is nonempty.

**Lemma 6.**

\( \forall \text{st}, c_1 \cdot (\text{st}, c_1) \in ((\text{st}_1 \| \text{cs}, c_2 \| \text{st}_2) \Rightarrow \text{st} \| \text{c} \text{cs} \neq \emptyset) \)

\( \land \text{st}_2 \| \text{c} \text{cs} \neq \emptyset \)

\( \text{provided } (\text{st}_1 \| \text{cs}, c_2 \| \text{st}_2) \neq \emptyset. \)

**Proof.** By induction.

**Case 1.**

\( \forall \text{st}, c_1 \cdot (\text{st}, c_1) \in ((\text{st}_1 \| \text{cs}, c_2 \| \text{st}_2) \Rightarrow \text{st} \| \text{c} \text{cs} \neq \emptyset) \)

\( \iff \) \( \color{red}{\text{false}} \) [definitions of \( ((\text{st}_1 \| \text{cs}, c_2 \| \text{st}_2) \rangle \text{cs} = \emptyset) \)]

\( \iff \) \( \langle \text{st} \| \text{c} \text{cs} \rangle \neq \emptyset \land \langle \text{st} \| \text{c} \text{cs} \rangle \neq \emptyset [\text{and } \langle \text{st} \| \text{c} \text{cs} \rangle \rangle \]

**Case 2.** \( d \not\in \text{cs} \)

\( \forall \text{st}, c_1 \cdot (\text{st}, c_1) \in ((\text{st}_1 \| \text{cs}, c_2 \| \text{st}_2) \Rightarrow \text{st} \| \text{c} \text{cs} \neq \emptyset) \)

\( \iff \) \( \color{red}{\text{false}} \) [definition of \( ((\text{st}_1 \| \text{cs}, c_2 \| \text{st}_2) \rangle \text{cs} = \emptyset, \text{if } d \not\in \text{cs} \)]

\( \iff \) \( \langle \text{st} \| \text{c} \text{cs} \rangle \neq \emptyset \land \langle \text{d}, \beta \rangle \| \text{c} \text{cs} \neq \emptyset \)

\( \langle \text{st} \| \text{c} \text{cs} \rangle \neq \emptyset \) and \( \langle \text{d}, \beta \rangle \| \text{c} \text{cs} \neq \emptyset \)

**Case 3.** \( d_1 \in \text{cs}, d_2 \not\in \text{cs} \)

\( \forall \text{st}, c_1 \cdot (\text{st}, c_1) \in ((\text{st}_1 \| \text{cs}, c_2 \| \text{st}_2) \Rightarrow \text{st} \| \text{c} \text{cs} \neq \emptyset) \)

\( \iff \) \( \forall \text{st}, c_1 \cdot (\text{st}, c_1) \in ((\text{st}_1 \| \text{cs}, c_2 \| \text{st}_2) \Rightarrow ((\text{d}_2, \beta) \land \text{st}_2) \| \text{c} \text{cs} \neq \emptyset) \)

\( [\text{definition of } ((\text{st}_1 \| \text{cs}, c_2 \| \text{st}_2) \rangle \text{cs} = \emptyset] \]

\( \iff \forall \text{st}, c_1 \cdot (\text{st}, c_1) \in ((\text{d}_1, \alpha) \land \text{st}_1) \| \text{c} \text{cs} \neq \emptyset \)

\( \langle \text{st} \| \text{c} \text{cs} \rangle \neq \emptyset \land \langle \text{d}_2, \alpha \rangle \| \text{c} \text{cs} \neq \emptyset \)

\( [\text{definition of } \langle \text{st} \| \text{c} \text{cs} \rangle \]
Case 4.: \( d \in cs \)
\[
\forall st, c_1 \cdot (st, c_1) \in (((d, \alpha) \bowtie st_1) [cs, c_2] ((d, \beta) \bowtie st_2)) \Rightarrow st \mid_C cs \neq \langle \rangle
\]
\[
\Leftrightarrow \forall st, c_1 \cdot (st, c_1) \in (st_1 \parallel cs, (c_2 \land \alpha = \beta)) \bowtie st_2 \Rightarrow ((d, \beta) \bowtie st) \mid_C cs \neq \langle \rangle
\]
[definition of \( ((d, \alpha) \bowtie st_1) \parallel cs, c_2 \parallel ((d, \beta) \bowtie st_2) \)]
\[
\Leftrightarrow true
\]
\[
[(d, \beta) \bowtie st] \mid_C cs \neq \langle \rangle \text{ by definition of } \mid_C
\]
\[
\Rightarrow ((d, \alpha) \bowtie st_1) \mid_C cs \neq \langle \rangle \land ((d, \beta) \bowtie st_2) \mid_C cs \neq \langle \rangle
\]
[definition of \( \mid_C \)]

Case 5.: \( d_1 \not\in cs, d_2 \not\in cs \)
\[
\forall st, c_1 \cdot (st, c_1) \in (((d_1, \alpha) \bowtie st_1) \parallel cs, c_2 \parallel ((d_2, \beta) \bowtie st_2)) \Rightarrow st \mid_C cs \neq \langle \rangle
\]
\[
\Leftrightarrow \forall st, c_1 \cdot (st, c_1) \in (((d_1, \alpha) \bowtie st_1) \parallel cs, c_2 \parallel ((d_2, \beta) \bowtie st_2)) \Rightarrow ((d_2, \beta) \bowtie st_2) \mid_C cs \neq \langle \rangle \land
\]
\[
((d_1, \alpha) \bowtie st_1) \mid_C cs \neq \langle \rangle \Rightarrow ((d_1, \alpha) \bowtie st_1) \mid_C cs \neq \langle \rangle
\]
[definition of \( ((d_1, \alpha) \bowtie st_1) \parallel cs, c_2 \parallel ((d_2, \beta) \bowtie st_2) \)]
\[
\Rightarrow \forall st, c_1 \cdot (st, c_1) \in (((d_1, \alpha) \bowtie st_1) \parallel cs, c_2 \parallel ((d_2, \beta) \bowtie st_2)) \Rightarrow ((d_2, \beta) \bowtie st_2) \mid_C cs \neq \langle \rangle \Rightarrow
\]
\[
((d_1, \alpha) \bowtie st_1) \mid_C cs \neq \langle \rangle \land ((d_2, \beta) \bowtie st_2) \mid_C cs \neq \langle \rangle
\]
[definition of \( \mid_C \)]

The following lemmas lift to the synchronisation operator for constrained symbolic traces results similar to some previously established for the operator for symbolic traces.

**Lemma 7.**
\[
\forall \alpha st \cdot \alpha st \in N^a \parallel (\alpha st_1 \parallel cs) \parallel \alpha st_2) \Rightarrow \alpha st \mid_C cs \neq \langle \rangle \Leftrightarrow \alpha st_1 \mid_C cs \neq \langle \rangle \land \alpha st_2 \mid_C cs \neq \langle \rangle
\]
where \( \alpha st_1 \leq a_1 \) and \( \alpha st_2 \leq a_2 \), and provided \( N^a \parallel (\alpha st_1 \parallel cs) \parallel \alpha st_2) \neq \emptyset \).

**Proof.**
\[
\forall \alpha st \cdot \alpha st \in N^a \parallel (\alpha st_1, c) \parallel cs \parallel (\alpha st_2, c) \parallel st) \Rightarrow \alpha st \mid_C cs \neq \langle \rangle
\]
\[
\Leftrightarrow \forall st, c \cdot (st, c) \in (\alpha st_1, c_1) \parallel cs \parallel (\alpha st_2, c_2) \parallel st) \Rightarrow (st, c) \mid_C cs \neq \langle \rangle
\]
[definition of \( N \)]
\[
\Leftrightarrow \forall st, c \cdot (st, c) \in (\alpha st_1, c_1) \parallel cs \parallel (\alpha st_2, c_2) \parallel st) \Rightarrow (st, c) \mid_C cs \neq \langle \rangle
\]
[definition of synchronising operator]
\[
\Rightarrow \forall st, c \cdot (st, c) \in (\alpha st_1, c_1) \parallel cs \parallel (\alpha st_2, c_2) \parallel st) \Rightarrow st \mid_C cs \neq \langle \rangle
\]
[definition of \( \mid_C \) for constrained symbolic traces]
\[
\Rightarrow st_1 \mid_C cs \neq \langle \rangle \land st_2 \mid_C cs \neq \langle \rangle
\]
[Lemma 6 and proviso]
\[
\Rightarrow (st_1, c_1) \mid_C cs \neq \langle \rangle \land (st_2, c_2) \mid_C cs \neq \langle \rangle
\]
[definition of \( \mid_C \) for constrained symbolic traces]

**Lemma 8.**
\[
\exists \alpha st \cdot \alpha st \in N^a \parallel (\alpha st_1 \parallel cs) \parallel \alpha st_2) \land \alpha st \mid_C cs \neq \langle \rangle
\]
\[
\Rightarrow \alpha st_1 \mid_C cs \neq \langle \rangle \land \alpha st_2 \mid_C cs \neq \langle \rangle \land \text{satisfiable}_{cs}(\alpha st_1, \alpha st_2)
\]

40
Proof.

\[ \exists \text{cst} \in \mathcal{N}^\alpha \left( (\text{st}_1, c_1) \left[ \text{cs} \right] (\text{st}_2, c_2) \right) \land \text{cst} \mid \text{cst} \neq \langle \rangle \]

\[ \Rightarrow \exists \text{st}, c \in (\text{st}_1, c_1) \left[ \text{cs} \right] (\text{st}_2, c_2) \land (\text{st}, c) \mid \text{cst} \neq \langle \rangle \]  
[definition of \( \mathcal{N} \)]

\[ \Rightarrow \exists \text{st}, c \in (\text{st}_1, c_1) \left[ \text{cs}, (c_1, c_2) \right] (\text{st}_2) \land (\text{st}, c) \mid \text{cst} \neq \langle \rangle \]  
[definition of synchronisation operator]

\[ \Rightarrow \exists \text{st}, c \in (\text{st}_1, c_1) \left[ \text{cs}, (c_1, c_2) \right] (\text{st}_2) \land (\text{st}, c) \mid \text{cst} \neq \langle \rangle \]  
[definition of \( \mid \text{cst} \) for constrained symbolic traces]

\[ \Rightarrow \text{st}_1 \mid \text{cst} \neq \langle \rangle \land \text{st}_2 \mid \text{cst} \land \text{satisfiable}_{\text{cst}}((\text{st}_1, c_1), (\text{st}_2, c_2)) \]  
[Lemma 11]

\[ \Rightarrow (\text{st}_1, c_1) \mid \text{cst} \neq \langle \rangle \land (\text{st}_2, c_2) \mid \text{cst} \land \text{satisfiable}_{\text{cst}}((\text{st}_1, c_1), (\text{st}_2, c_2)) \]  
[definition of \( \mid \text{cst} \) for constrained symbolic traces]

The lemma below establishes that the traces built from the (local) traces of \( P_1 \) and \( P_2 \), are all those of the parallelism between \( P_1 \) and \( P_2 \).

**Lemma 9.** For every pair of disjoint alphabets \( a_1 \) and \( a_2 \)

\[ \text{cstraces}^a(P_1 \left[ \text{cs} \right] P_2) = \bigcup \{ \text{cstraces}^a(P_1) ; \text{cstraces}^a(P_2) \} \subseteq \mathcal{N}^\alpha \left( (\text{st}_1, c_1) \left[ \text{cs} \right] (\text{st}_2, c_2) \right) \]

**Proof.** In giving the semantics of \( P_1 \left[ \text{cs} \right] P_2 \), we observe that we can assume, without loss of generality, that

\[ P_1 = \text{begin state} [x_1 : T_1] \bullet A_1 \text{ end and } P_2 = \text{begin state} [x_2 : T_2] \bullet A_2 \text{ end} \]

with \( x_1 \cap x_2 = \varnothing \), where \( x_1 \) and \( x_2 \) are the lists of state components of \( P_1 \) and \( P_2 \), and for simplicity, we sometimes use \( x_1 \) and \( x_2 \) as sets of variable names.

\[ \text{cstraces}^a(P_1 \left[ \text{cs} \right] P_2) \]

\[ = \text{cstraces}^a(\text{begin state} [x_1 : T_1 ; x_2 : T_2] \bullet A_1 \left[ x_1 \mid x_2 \right] A_2 \text{ end}) \quad \text{[semantics of process parallelism]} \]

\[ = \text{cstraces}^a(\forall \text{st_1} \in T_1 \land \forall \text{st_2} \in T_2 \land \forall x_1, x_2 : \text{st_1}, \text{st_2} \mid x_1 \mid x_2) \]

\[ \text{cstraces}^a(\forall \text{st_1}, \text{st_2} \mid x_1 \mid x_2) \]

\[ \Rightarrow \{ \text{st}, c_2, s_2, A_3 \mid \text{ast} \leq a \land \]

\[ \forall \text{w_1} \in T_1 \land \forall \text{w_2} \in T_2 \land \forall x_1, x_2 : \text{st_1}, \text{st_2} \mid x_1 \mid x_2) \]

\[ \Rightarrow \{ \text{st}, c_2, s_2, A_3 \mid \text{ast} \leq a \land \]

\[ \exists \text{st_1}, c_1', s_1', A_1', \text{st_2}, c_2', s_2', A_2' \bullet \]

\[ \forall \text{st_1} \in T_1 \land \forall \text{st_2} \in T_2 \land \forall x_1, x_2 : \text{st_1}, \text{st_2} \mid x_1 \mid x_2) \]

\[ \Rightarrow \{ \text{st}, c_2, s_2, A_3 \mid \text{ast} \leq a \land \]

\[ \exists \text{st_1}, c_1', s_1', A_1', \text{st_2}, c_2', s_2', A_2' \bullet \]

\[ \forall \text{st_1} \in T_1 \land \forall \text{st_2} \in T_2 \land \forall x_1, x_2 : \text{st_1}, \text{st_2} \mid x_1 \mid x_2) \]

\[ \Rightarrow \{ \text{st}, c_2, s_2, A_3 \mid \text{ast} \leq a \land \]

\[ \exists \text{st_1}, c_1', s_1', A_1', \text{st_2}, c_2', s_2', A_2' \bullet \]

\[ \forall \text{st_1} \in T_1 \land \forall \text{st_2} \in T_2 \land \forall x_1, x_2 : \text{st_1}, \text{st_2} \mid x_1 \mid x_2) \]

\[ \Rightarrow \{ \text{st}, c_2, s_2, A_3 \mid \text{ast} \leq a \land \]

\[ \exists \text{st_1}, c_1', s_1', A_1', \text{st_2}, c_2', s_2', A_2' \bullet \]

\[ \forall \text{st_1} \in T_1 \land \forall \text{st_2} \in T_2 \land \forall x_1, x_2 : \text{st_1}, \text{st_2} \mid x_1 \mid x_2) \]
\[\{\text{st}, c_2\} \quad \exists \text{st}_1, c'_1, s'_1, A'_1, \text{st}_2, c'_2, s'_2, A'_2 \quad \text{with} \quad (w_1 \in T_1 \land w_2 \in T_2 \mid x_1 := w_1 \models A_1) \overset{\text{st}_1}{\Rightarrow} (c'_1' \mid s'_1' \models A'_1') \land \\
(w_1 \in T_1 \land w_2 \in T_2 \mid x_2 := w_2 \models A_2) \overset{\text{st}_2}{\Rightarrow} (c'_2' \mid s'_2' \models A'_2') \land \\
\alpha c'_1 \cap \alpha c'_2 = \emptyset \land \text{ast}_1 \subseteq \alpha c'_1 \land \text{ast}_2 \subseteq \alpha c'_2 \land \\
\mathcal{R}(\text{st}, c_2) \in \mathcal{N}^\alpha (\mathcal{R} \circ \text{st}_1 \lbrack \text{cs}, (c'_1' \land c'_2') \lbrack \text{st}_2]) \]

- \(\mathcal{R}(\text{st}, c_2)\)

\[\{\text{st}, c_2\} \quad \exists \text{st}_1, c'_1, \text{st}_2, c'_2, b_1, b_2 \quad \text{with} \quad (w_1 \in T_1 \mid x_1 := w_1 \models A_1) \overset{\text{st}_1}{\Rightarrow} (c'_1 \mid s'_1 \models A'_1) \land \\
(w_1 \in T_1 \mid x_2 := w_2 \models A_2) \overset{\text{st}_2}{\Rightarrow} (c'_2 \mid s'_2 \models A'_2) \land \\
\alpha c'_1 \cap \alpha c'_2 = \emptyset \land \text{ast}_1 \subseteq \alpha c'_1 \land \text{ast}_2 \subseteq \alpha c'_2 \land \\
\mathcal{R}(\text{st}, c_2) \in \mathcal{N}^\alpha (\mathcal{R} \circ \text{st}_1 \lbrack \text{cs}, (c'_1 \land c'_2) \lbrack \text{st}_2]) \]

- \(\mathcal{R}(\text{st}, c_2)\)

\[\{\text{st}, c_2\} \quad \exists \text{st}_1, c'_1, \text{st}_2, c'_2, b_1, b_2 \quad \text{with} \quad (w_1 \in T_1 \mid x_1 := w_1 \models A_1) \land \alpha c'_1 \cap \alpha c'_2 = \emptyset \land \text{ast}_1 \subseteq \alpha c'_1 \land \text{ast}_2 \subseteq \alpha c'_2 \land \\
\mathcal{R}(\text{st}, c_2) \in \mathcal{N}^\alpha (\mathcal{R} \circ \text{st}_1 \lbrack \text{cs}, (\exists x_1 \cdot c'_1) \lbrack \text{st}_2]) \]

- \(\mathcal{R}(\text{st}, c_2)\)

\[\{\text{st}, c_2\} \quad \exists \text{st}_1, c'_1, \text{st}_2, c'_2, b_1, b_2 \quad \text{with} \quad (w_1 \in T_1 \mid x_1 := w_1 \models A_1) \land \alpha c'_1 \cap \alpha c'_2 = \emptyset \land \text{ast}_1 \subseteq \alpha c'_1 \land \text{ast}_2 \subseteq \alpha c'_2 \land \\
\mathcal{R}(\text{st}, c_2) \in \mathcal{N}^\alpha (\mathcal{R} \circ \text{st}_1 \lbrack \text{cs}, (\exists x_2 \cdot c'_2) \lbrack \text{st}_2]) \]

- \(\mathcal{R}(\text{st}, c_2)\)

\[\{\text{st}, c_2\} \quad \exists \text{st}_1, c'_1, \text{st}_2, c'_2, b_1, b_2 \quad \text{with} \quad (w_1 \in T_1 \mid x_1 := w_1 \models A_1) \land \alpha c'_1 \cap \alpha c'_2 = \emptyset \land \text{ast}_1 \subseteq \alpha c'_1 \land \text{ast}_2 \subseteq \alpha c'_2 \land \\
\mathcal{R}(\text{st}, c_2) \in \mathcal{N}^\alpha (\mathcal{R} \circ \text{st}_1 \lbrack \text{cs}, \emptyset \lbrack \text{st}_2]) \]

- \(\mathcal{R}(\text{st}, c_2)\)

\[\{\text{st}, c_2\} \quad \exists b_1, b_2 \quad \text{with} \quad \text{disjoint}(b_1, b_2) \land \mathcal{R}(\text{st}, c_2) \in \mathcal{N}^\alpha (\mathcal{R} \circ \text{st}_1 \lbrack \text{cs}, \emptyset \lbrack \text{st}_2]) \]

- \(\mathcal{R}(\text{st}, c_2)\)
\[
\text{Case 2.} \\
\text{Proof.} \quad \text{Lemma 11.} \text{not only is not empty, but also contains at least one trace with at least one synchronisation. This relationship between the notion of satisfiability and the existence of synchronisation traces reassures us of the adequacy of the definition of satisfiability.}
\]

\text{Appendix C.2. Properties of satisfiability}

Satisfiability, as captured by \text{satisfiable}_{cs}((\text{st}_1, c_1), (\text{st}_2, c_2)), does not ensure that there is an actual synchronisation arising from the traces \text{st}_1 and (\text{st}_2, since their projections (\text{st}_1 | E cs) and (\text{st}_2 | E cs) might be empty. It does ensure, however, that the set of traces defined by the synchronisation operator is not empty. This is established by the Lemma 10 proved below.}

\text{Lemma 10.} \quad (\text{st}_1 \sqsubseteq \text{cs}, (c_1 \land c_2) \sqsubseteq \text{st}_2) \neq \emptyset \iff \text{satisfiable}_{cs}((\text{st}_1, c_1), (\text{st}_2, c_2))

\text{Proof.} \quad (\text{st}_1 \sqsubseteq \text{cs}, (c_1 \land c_2) \sqsubseteq \text{st}_2) \neq \emptyset \\
\quad \iff \exists a_1, a_2 \cdot (\text{st}_1 | E cs) = a_5 (\text{st}_2 | E cs) \land c_1 \land c_2 \quad \quad \text{[Lemma 5, with \alpha \text{st}_1 \leq a_1 and \alpha \text{st}_2 \leq a_2]} \\
\quad \iff \text{satisfiable}_{cs}((\text{st}_1, c_1), (\text{st}_2, c_2)) \quad \quad \text{[definition of satisfiable]}
\]

This relationship between the notion of satisfiability and the existence of synchronisation traces reassures us of the adequacy of the definition of satisfiability.

The following lemma identifies a stronger condition that holds when the set of synchronisation traces not only is not empty, but also contains at least one trace with at least one synchronisation.

\text{Lemma 11.} \quad \exists \text{st}, c \cdot (\text{st}, c) \in (\text{st}_1 \sqsubseteq \text{cs}, (c_1 \land c_2) \sqsubseteq \text{st}_2) \land \text{st} | c \text{ cs} \neq \emptyset \\
\quad \Rightarrow \text{st}_1 | c \text{ cs} \neq \emptyset \land \text{st} | c \text{ cs} \neq \emptyset \land \text{satisfiable}_{cs}((\text{st}_1, c_1), (\text{st}_2, c_2))

\text{Proof.} \quad \text{By induction.}

\text{Case 1.} \quad \exists \text{st}, c \cdot (\text{st}, c) \in ((\text{st}_1 \sqsubseteq \text{cs}, (c_1 \land c_2) \sqsubseteq \text{st}_2) \land \text{st} | c \text{ cs} \neq \emptyset) \\
\quad \Rightarrow \text{false} \quad \quad \quad \quad \quad \quad \quad \quad \text{[definitions of (\text{st}, c, c_2 \sqsubseteq \text{st}_2) \land \text{st} | c \text{ cs} \neq \emptyset]} \\
\quad \Rightarrow (\text{st} | c \text{ cs} \neq \emptyset) \land (\text{st} | c \text{ cs} \neq \emptyset) \land \text{satisfiable}_{cs}((\text{st}_1, c_1), (\text{st}_2, c_2)) \quad \quad \quad \quad \quad \quad \quad \quad \text{[} (\text{st} | c \text{ cs} = \emptyset) \text{]} \\
\text{Case 2.} \quad : d \notin \text{cs} \\
\exists \text{st}, c \cdot (\text{st}, c) \in ((\text{st}_1 \sqsubseteq \text{cs}, (c_1 \land c_2) \sqsubseteq (d, \beta) \sqsubseteq \text{st}_2) \land \text{st} | c \text{ cs} \neq \emptyset) \\
\quad \Rightarrow \text{false} \quad \quad \quad \quad \quad \quad \quad \quad \text{[definition of ((\text{st} | c, d, \beta) \sqsubseteq \text{st}_2) \land (d, \beta) | c \text{ cs} = \emptyset, if d \notin \text{cs}]} \\
\quad \Rightarrow (\text{st} | c \text{ cs} \neq \emptyset) \land (d, \beta) | c \text{ cs} \neq \emptyset \land \text{satisfiable}_{cs}((\text{st}_1, c_1), (d, \beta, c_2)) \quad [ (\text{st} | c \text{ cs} = \emptyset) \land (d, \beta) | c \text{ cs} = \emptyset])
Case 3.: \( d_1 \in cs, d_2 \notin cs \)

\[(\exists st, c \in (\langle (d_1, o) \land st_1 \rangle \| \langle (c, c_1 \land c_2) \| (d_2, o) \land st_2 \rangle) \land st \| c cs \neq \langle \rangle) \]
\[\Leftrightarrow (\exists st, c \in (\langle (d_1, o) \land st_1 \rangle \| \langle (c, c_1 \land c_2) \| st_2 \rangle \land (d_2, o) \land st) \| c cs \neq \langle \rangle) \]
\[\Leftrightarrow (\langle (d_1, o) \land st_1 \rangle \| c cs \neq \langle \rangle) \land st \| c cs \neq \langle \rangle \]
\[\Leftrightarrow (\langle (d_1, o) \land st_1 \rangle \| c cs \neq \langle \rangle) \land satisfies_{c_2}(\langle (d_1, o) \land st_1 \rangle, (c, c_1 \land c_2)) \]

Case 4.: \( d \in cs \)

\[(\exists st, c \in (\langle (d, o) \land st_1 \rangle \| \langle (c, c_1 \land c_2) \| (d_2, o) \land st_2 \rangle) \land st \| c cs \neq \langle \rangle) \]
\[\Leftrightarrow (\exists st, c_1 \in (st \| c cs \neq \langle \rangle) \land (d_2, o) \land st \| c cs \neq \langle \rangle) \]
\[\Leftrightarrow (\langle (d_1, o) \land st_1 \rangle \| c cs \neq \langle \rangle) \land satisfies_{c_2}(\langle (d_1, o) \land st_1 \rangle, (c, c_1 \land c_2)) \]

Case 5.: \( d_1 \neq d_2, d_1 \in cs, d_2 \in cs \)

\[(\exists st, c \in (\langle (d_1, o) \land st_1 \rangle \| \langle (c, c_1 \land c_2) \| (d_2, o) \land st_2 \rangle) \land st \| c cs \neq \langle \rangle) \]
\[\Leftrightarrow false \]
\[\Leftrightarrow (\langle (d_1, o) \land st_1 \rangle \| c cs \neq \langle \rangle) \land satisfies_{c_2}(\langle (d_1, o) \land st_1 \rangle, (d_2, o) \land st_2) \]

[definition of satisfies and \( |E | \)]
Case 6: $d_1 \not\in cs, d_2 \not\in cs$

$$\exists st, c \cdot (st, c) \in \{(d_1, \alpha) \cap st_1) [\mathcal{N}(c, (c_1 \land c_2)] ((d_2, \beta) \cap st_2)) \land st \models cs \not= \langle \rangle$$

$$\iff (\exists st, c \cdot (st, c_1) \in \{(d_1, \alpha) \cap st_1) [\mathcal{N}(c, (c_1 \land c_2)] ((d_2, \beta) \cap st) \models cs \not= \langle \rangle)$$

$$\lor (\exists st, c \cdot (st, c) \in (st_1 [\mathcal{N}(c, (c_1 \land c_2)] ((d_2, \beta) \cap st_2)) \land (d_1, \alpha) \cap st) \models cs \not= \langle \rangle)$$

[definition of $(d_1, \alpha) \cap st_1) [\mathcal{N}(c, c_2] ((d_2, \beta) \cap st_2))]$]

$$\iff ((d_1, \alpha) \cap st_1) \models cs \not= \langle \rangle \land st_2 \models cs \not= \langle \rangle \land satisifable cs(((d_1, \alpha) \cap st_1, c_1), (st_2, c_2)) \lor$$

$$(st_1 \models cs \not= \langle \rangle \land (d_2, \beta) \cap st_2) \models cs \not= \langle \rangle \land satisifable cs((st_1, c_1), (d_2, \beta) \cap st_2, c_2))$$

[induction hypothesis]

The reverse implication is a direct consequence of Lemmas 10 and 6.

Appendix C.3. Properties of normalisation

When applied to equivalent constrained symbolic traces, $\mathcal{N}$ makes them syntactically equal.

**Lemma 12.**

$$\text{cst}_1 \equiv \text{cst}_2 \Rightarrow \mathcal{N}(\text{cst}_1) = \mathcal{N}(\text{cst}_2)$$

**Proof.** Direct from the definition of $\mathcal{N}$ and equivalence of constrained symbolic traces: $(st_1, c_1) \equiv (st_2, c_2)$ if and only if $st_1 \models cs = st_1 \models cs$ and $c_1 \models (cs) = c_2$. The projection operation $st \models cs$ keeps just the channels of the trace $st$. □

The following lemma gives a property of alphabets and $\mathcal{N}$.

**Lemma 13.** For every $a_1$ and $a_2$ such that $ast \leq a_1$ and $ast \leq a_2$,

$$(st, c) = \mathcal{N}^{a_1}(cst) \iff (st, c) = \mathcal{N}^{a_2}(cst)$$

**Proof.**

$$(st, c) = \mathcal{N}^{a_1}(st_1, c_1)$$

$$\iff (st = st_1[a_1/ast]) \land (c = c_1[a_1/ast]) \quad \text{[definition of $\mathcal{N}^{a_1}$]}$$

$$\iff (st = st_1[a_2/ast]) \land (c = c_1[a_2/ast]) \quad \text{[ost \leq a_1 and ast \leq a_2 imply (a_1 | \# st) \leq a_2]}$$

$$\iff (st, c) = \mathcal{N}^{a_2}(st_1, c_1) \quad \text{[definition of $\mathcal{N}^{a_2}$]}$$

We use $(a | \# n)$ to refer to the first $n$ elements of the alphabet $a$, and $\# st$ for the size of a trace $st$. □
Appendix D. Proofs of theorems

Theorem 2.

\[\text{Scstraces}^{a_{1}, a_{2}}_{\text{cs}}(P_1, P_2) = \{ \text{cs} : \text{cstraces}^{a_2}(P_1 [ \text{cs} ] P_2) | \text{cs} \upharpoonright_c \text{cs} \neq \langle \rangle \}\]

Proof.

\[\text{Scstraces}^{a_{1}, a_{2}}_{\text{cs}}(P_1, P_2) = \bigcup \{ p : \text{Sctrace}^{P(P_1, P_2)}_{\text{cs}}(P_1, P_2) \} \bullet N^a(\{ p.1 [\text{cs}] p.2 \}) \]  

[definition of Scstraces]

\[= \bigcup \{ \text{cst}_1 : \text{cstraces}^{a_2}(P_1) ; \text{cst}_2 : \text{cstraces}^{a_2}(P_2) | (\text{cst}_1 \upharpoonright_c \text{cs}) \neq \langle \rangle \land (\text{cst}_2 \upharpoonright_c \text{cs}) \neq \langle \rangle \land \text{satisfiable}_{\text{cs}}(\text{cst}_1, \text{cst}_2) \}
\bullet N^a(\{\text{cst}_1 [\text{cs} ] \text{cst}_2\}) \]  

[definition of SctraceP]  

\[= \{ \text{cst}_1 : \text{cstraces}^{a_2}(P_1) ; \text{cst}_2 : \text{cstraces}^{a_2}(P_2) | (\text{cst}_1 \upharpoonright_c \text{cs}) \neq \langle \rangle \land (\text{cst}_2 \upharpoonright_c \text{cs}) \neq \langle \rangle \land \text{satisfiable}_{\text{cs}}(\text{cst}_1, \text{cst}_2) \} \]  

[property of sets]

\[= \{ \text{cst}_1 : \text{cstraces}^{a_2}(P_1) ; \text{cst}_2 : \text{cstraces}^{a_2}(P_2) | (\text{cst}_1 \upharpoonright_c \text{cs}) \neq \langle \rangle \land (\text{cst}_2 \upharpoonright_c \text{cs}) \neq \langle \rangle \land \text{satisfiable}_{\text{cs}}(\text{cst}_1, \text{cst}_2) \} \]  

• \text{cst}  

\[= \{ \text{cst}_1 : \text{cstraces}^{a_2}(P_1) ; \text{cst}_2 : \text{cstraces}^{a_2}(P_2) | (\text{cst}_1 \upharpoonright_c \text{cs}) \neq \langle \rangle \land (\text{cst}_2 \upharpoonright_c \text{cs}) \neq \langle \rangle \land \text{satisfiable}_{\text{cs}}(\text{cst}_1, \text{cst}_2) \} \]  

[Lemma 8 and 7]

\[= \{ \text{cst}_1 : \text{cstraces}^{a_2}(P_1) ; \text{cst}_2 : \text{cstraces}^{a_2}(P_2) | (\text{cst}_1 \upharpoonright_c \text{cs}) \neq \langle \rangle \land (\text{cst}_2 \upharpoonright_c \text{cs}) \neq \langle \rangle \} \]  

[Lemma 9]  

\[= \{ \text{cst} : \text{cstraces}^{a_2}(P_1 \ [ \text{cs} ] P_2) | \text{cst} \upharpoonright_c \text{cs} \neq \langle \rangle \} \]  

\[\square\]

Theorem 3.

\[\text{Scstraces}^{a_{1}}_{\text{cs}}(\text{Scstraces}^{a_{2}}_{\text{cs}}(\text{cstraces}^{a_1}(P_1), \text{cstraces}^{a_2}(P_2)), \text{cstraces}^{a_1}(P_3)) = \text{Scstraces}^{a_{1}}_{\text{cs}}(\text{cstraces}^{a_1}(P_1 \ [ \text{cs} ] P_2), \text{cstraces}^{a_1}(P_3)) \]

Proof.

\[\text{Scstraces}^{a_{1}}_{\text{cs}}(\text{Scstraces}^{a_{2}}_{\text{cs}}(\text{cstraces}^{a_1}(P_1), \text{cstraces}^{a_2}(P_2)), \text{cstraces}^{a_1}(P_3)) = \text{Scstraces}^{a_{1}}_{\text{cs}}(\bigcup \{ p : \text{Sctrace}^{P(P_1, P_2)}_{\text{cs}}(P_1, P_2) \} \bullet N^{a_{12}}(\{ p.1 [\text{cs}] p.2 \}), \text{cstraces}^{a_1}(P_3)) \]  

[Definition 25]

\[= \text{Scstraces}^{a_{1}}_{\text{cs}}(\bigcup \{ \text{cst}_1 : \text{cstraces}^{a_1}(P_1) ; \text{cst}_2 : \text{cstraces}^{a_2}(P_2) | (\text{cst}_1 \upharpoonright_c \text{cs}) \neq \langle \rangle \land (\text{cst}_2 \upharpoonright_c \text{cs}) \neq \langle \rangle \land \text{satisfiable}_{\text{cs}}(\text{cst}_1, \text{cst}_2) \}
\bullet N^{a_{12}}(\{\text{cst}_1 [\text{cs} ] \text{cst}_2\}) \], \text{cstraces}^{a_1}(P_3)) \]  

[Definition 24]

\[= \text{Scstraces}^{a_{1}}_{\text{cs}}(\bigcup \{ p : \text{Sctrace}^{P(P_1, P_2)}_{\text{cs}}(P_1, P_2) \} \bullet N^{a_{12}}(\{ p.1 [\text{cs}] p.2 \}), \text{cstraces}^{a_1}(P_3)) \]  

[Definition 12]

\[= \text{Scstraces}^{a_{1}}_{\text{cs}}(\text{Scstraces}^{a_{1}}_{\text{cs}}(P_1, P_2), \text{cstraces}^{a_1}(P_3)) \]  

[Definition 15]

\[= \text{Scstraces}^{a_{1}}_{\text{cs}}(\{ \text{cst} : \text{cstraces}^{a_1}(P_1 \ [ \text{cs} ] P_2) | \text{cst} \upharpoonright_c \text{cs} \neq \langle \rangle \}, \text{cstraces}^{a_1}(P_3)) \]  

[Theorem 2]

\[= \text{Scstraces}^{a_{1}}_{\text{cs}}(\{ \text{cst} : \text{cstraces}^{a_1}(P_1 \ [ \text{cs} ] P_2) | \text{cst} \upharpoonright_c \text{cs} \neq \langle \rangle \}, \text{cstraces}^{a_1}(P_3)) \bullet N^{a_{1}}(\{ p.1 [\text{cs}] p.2 \}) \]  

\[46\]
By induction.

Proof. We can assume, without loss of generality, that

Case: choices. We can assume, without loss of generality, that

\[ \text{selectS}^a(P_1) \subseteq \text{cstraces}^a(P) \]

Theorem 4.

Proof. By induction.

Case: basic process. Trivial, because \( \text{selectS}(P) = \emptyset \).

Case: parallelism. Direct consequence of Theorem 2.

Case: choices. We can assume, without loss of generality, that

\[ P_1 = \text{begin state} [x_1 : T_1] \bullet A_1 \text{ end} \quad \text{and} \quad P_2 = \text{begin state} [x_2 : T_2] \bullet A_2 \text{ end} \]

with \( x_1 \cap x_2 = \emptyset \), where \( x_1 \) and \( x_2 \) are the lists of state components of \( P_1 \) and \( P_2 \), and for simplicity, we sometimes use \( x_1 \) and \( x_2 \) as sets of variable names.

\[ \text{selectS}^a(P_1 \sqcup P_2) \]

\[ \subseteq \text{cstraces}^a(P_1) \cup \text{cstraces}^a(P_2) \]

\[ \subseteq \text{cstraces}^a(w_1 \in T_1, x_1 := w_1, A_1) \cup \text{cstraces}^a(w_2 \in T_2, x_2 := w_2, A_2) \]

[definition of \( \text{cstraces} \)]

\[ \subseteq \text{cstraces}^a(w_1 \in T_1 \land w_2 \in T_2, (x_1, x_2 := w_1, w_2), A_1) \cup \text{cstraces}^a(w_1 \in T_1 \land w_2 \in T_2, (x_1, x_2 := w_1, w_2), A_2) \]

[definition of \( \text{cstraces} \), and Propositions 1 and 2]

\[ = \left\{ \begin{array}{l} \text{st}, c_3, s_3, A_3 \mid c_3 \leq a \land (w_1 \in T_1 \land w_2 \in T_2) \land x_1, x_2 := w_1, w_2 \models A_1 \rightarrow (c_3, s_3, A_3) \models R(\text{st}, c_2) \\ \text{st}, c_3, s_3, A_3 \mid c_3 \leq a \land (w_1 \in T_1 \land w_2 \in T_2) \land x_1, x_2 := w_1, w_2 \models A_2 \rightarrow (c_3, s_3, A_3) \models R(\text{st}, c_3) \end{array} \right\} \]

47
We can assume, without loss of generality, that Case: sequence. 

\[
\text{selectS}^a(P_1; P_2) = selectS^a(P_1) \cup N^a(\text{tcstraces}^a(P_1) \text{ cat selectS}^a(P_2)) \subseteq \text{cstraces}^a(w_1 \in T_1, x_1 := w_1, A_1) \cup N^a(\text{tcstraces}^a(w_1 \in T_1, x_1 := w_1, A_1) \text{ cat cstraces}^a(w_2 \in T_2, x_2 := w_2, A_2))
\]

The proof is similar for internal choice.

Case: sequence. We can assume, without loss of generality, that

\[
P_1 = \text{begin state } [x_1 : T_1] \bullet A_1 \text{ end and } P_2 = \text{begin state } [x_2 : T_2] \bullet A_2 \text{ end}
\]

with \(x_1 \cap x_2 = \emptyset\), where \(x_1\) and \(x_2\) are the lists of state components of \(P_1\) and \(P_2\), and for simplicity, we sometimes use \(x_1\) and \(x_2\) as sets of variable names.

\[
\text{selectS}^a(P_1; P_2) = selectS^a(P_1) \cup N^a(\text{tcstraces}^a(P_1) \text{ cat selectS}^a(P_2))
\]

[definition of \(cstraces\)]

[property of sets]

\[
= \{ st, c_3, s_3, A_3 | \text{ast} \leq a \wedge (w_1 \in T_1 \wedge w_2 \in T_2 | x_1, x_2 := w_1, w_2 \models A_1) \xrightarrow{st} (c_3 | s_3 \models A_3) \}
\]

[definitions of \(cstraces\) and \(testraces\)]

[Proposition 4]

[definition of \(cstraces\)]

[definition of \(estraces\)]

[definition of process external choice and \(cstraces\)]

[Proposition 4]

[Proposition 2]
= \{ \text{st, } c_3, s_3, A_3 \mid \text{ost} \leq a \land (w_1 \in T_1 \land w_2 \in T_2 \mid x_1, x_2 := w_1, w_2 \models A_1) \xrightarrow{\text{st}} (c_3 \mid s_3 \models A_3) \} \cup \\
\{ \text{st, st}_1, c_2, s_2, st_2, c_3, s_3, A_3 \mid \\
\text{ost}_1 \leq a_1 \land (w_1 \in T_1 \land w_2 \in T_2 \mid x_1, x_2 := w_1, w_2 \models A_1) \xrightarrow{\text{st}} (c_2 \mid s_2 \models \text{Skip}) \land \\
\text{ost}_2 \leq a_2 \land (c_2 \times s_2 \models A_2) \xrightarrow{\text{st}} (c_3 \mid s_3 \models A_3) \\
\} \cup \\
\{ \text{st, st}_1, c_2, s_2, st_2, c_3, s_3, A_3 \mid \\
\text{st} = \text{st}_1 \cap \text{st}_2 \land \text{ost}_1 \leq a_1 \land \text{ost}_2 \leq a_2 \land \\
(w_1 \in T_1 \land w_2 \in T_2 \mid x_1, x_2 := w_1, w_2 \models A_1) \xrightarrow{\text{st}} (c_2 \mid s_2 \models \text{Skip}) \land \\
{c_2 \mid s_2 \models A_2} \xrightarrow{\text{st}} (c_3 \mid s_3 \models A_3) \\
\} \cup \\
\{ \text{st, st}_1, c_2, s_2, st_2, c_3, s_3, A_3 \mid \\
\text{ost} \leq a \land \left( \text{st} = \text{st}_1 \cap \text{st}_2 \land \text{ost}_1 \leq a_1 \land \text{ost}_2 \leq a_2 \land \\
(w_1 \in T_1 \land w_2 \in T_2 \mid x_1, x_2 := w_1, w_2 \models A_1) \xrightarrow{\text{st}} (c_2 \mid s_2 \models \text{Skip}) \land \\
(c_2 \mid s_2 \models A_2) \xrightarrow{\text{st}} (c_3 \mid s_3 \models A_3) \right) \\
\} \cup \\
\{ \text{st, c_3, s_3, A_3} \mid \text{ost} \leq a \land (w_1 \in T_1 \land w_2 \in T_2 \mid x_1, x_2 := w_1, w_2 \models A_1) \xrightarrow{\text{st}} (c_3 \mid s_3 \models A_3) \} \\
\} \\
\} \\
\} \\
\}
Case: hiding. We can assume, without loss of generality, that 

\[ P = \text{begin state } [x : T] \bullet A \text{ end} \]

selectS^a(P_1 \setminus cs)

\[= \mathcal{N}^a \langle \langle \text{selectS}^a(P) \rangle \rangle |_{ccs} \]

\[\subseteq \mathcal{N}^a \langle \langle \text{eetraces}^a(P) \rangle \rangle |_{ccs} \]

\[= \mathcal{N}^a \langle \langle \text{eetraces}^a(w \in T, x := w, A) \rangle \rangle |_{ccs} \]

\[= \{ \text{cst} : \text{eetraces}^a(w \in T, x := w, A) \bullet \mathcal{N}^a(\text{cst} \downarrow ccs) \} \]

\[= \{ \text{cst} : \text{eetraces}^a(w \in T, x := w, A) \bullet \mathcal{N}^a(R(st, c_s) \downarrow ccs) \} \]

\[= \{ \text{cst} : \text{eetraces}^a(P_1 \setminus cs) \} \]

□