ELSEVIER

Theoretical Computer Science 266 (2001) 237–248

Theoretical Computer Science

www.elsevier.com/locate/tcs

Divergence in testing and readiness semantics

Michele Boreale, Rocco De Nicola, Rosario Pugliese *

Dipartimento di Sistemi e Informatica, Università di Firenze, Via Lombroso 6/17, I-50134 Firenze, Italy

Received October 1998; revised July 1999; accepted February 2000

Abstract

Many variants of must-testing semantics have been put forward that are equally sensitive to deadlock, but differ for the stress they put on divergence, i.e. on the possibility for systems of getting involved in infinite internal computations. *Safe-testing* is one such variant, that naturally pops up when studying the behavioural pre-congruences induced by certain basic observables. Here, we study the relationship between safe-testing and Olderog's *readiness semantics*, a semantics induced by a natural process logic. We show that safe-testing is finer than readiness, and coincides with a refinement of readiness obtained by tuning Olderog's definition. For both safe-testing and the original readiness semantics we propose simple complete axiomatizations, which permit a fuller appreciation of their similarities and differences.

Keywords: Readiness semantics; Divergence; Safe-testing

1. Introduction

Divergence represents the possibility for a system of getting involved in an infinite sequence of internal communications. Since divergence could lead a system to ignoring all subsequent external stimuli, it plays a central role in the semantics of process description languages.

In [1] we have studied the different equivalences obtained by considering the maximal precongruences induced over TCCS [4] by three basic observables (predicates), two of which are based on divergence:

- $P\downarrow$ tests whether a process cannot get involved in an infinite sequence of internal actions (*converges*);
- $P\downarrow\ell$ tests whether a process converges and does so also after performing the specific action ℓ;

* Corresponding author.
E-mail address: pugliese@dsi.unifi.it (R. Pugliese).

0304-3975/01/$ - see front matter
PII: S0304-3975(00)00170-5

- $P\,!\ell$ tests whether a process, by internal actions, can only reach states from which action ℓ can be performed.

We have shown that the three predicates above naturally induce five contextual preorders, four of which coincide with well-known behavioural preorders over processes studied in the literature. In particular, the contextual preorder induced by $!\ell$ coincides with the pre-congruence induced by the *fair/should* preorder of [2, 9] and the contextual preorder induced by $\downarrow$ and $!\ell$ coincides with $\sqsubseteq_M$, the original *must* preorder of [3, 5].

When considering the conjunction of $\downarrow\ell$ and $!\ell$, a new preorder pops up, that we named *safe-must*, $\sqsubseteq_{SM}$. This preorder is supported by an intuitive testing scenario, where a computation from a pair observer-process is deemed successful if a success state is reached *strictly before* a "catastrophic" (divergent) one. This condition is stronger than the one considered by De Nicola and Hennessy [3] and amounts to requiring that the observed process does not diverge even after the final communication that takes the observer to success. The adjective *safe* is there to suggest that one can "safely" aim at success.

Olderog, in [10], introduces a similar requirement (*must engage*) and uses it in conjunction with other conditions to define when a process satisfies a set of logical formulae expressing a trace specification. This logical notion is then proven to be in full agreement with a set–theoretic definition of *readiness semantics*, in the sense that two processes have the same semantics if and only if they satisfy the same set of logical formulae.

As an example, both readiness equivalence and safe-testing validate the equality $a.\Omega = a.\Omega \oplus \mathbf{0}$. Reading from left to right, this can be explained by saying that an unsafe action (the a leading to Ω – divergence) cannot be guaranteed, due to the possibility of deadlock introduced by the internal choice $\oplus$. This is in sharp contrast with both must [3] and fair testing [2, 9].

Here, we make the relationship between safe-testing and readiness semantics precise. In particular,

- we show that safe-testing is finer than readiness, and coincides with a tuning of Olderog's definition;
- we present complete axiomatizations for both safe-testing and the original readiness semantics.

Interestingly, each of the two axiomatizations is obtained by adding a single new law to an axiomatization of must testing (see, e.g., [5]). This permits a full appreciation of the similarities between the three semantics, and highlights the central role played by the original testing theory.

As a base language, we shall consider a simple variant of CCS, named Tau-less CCS (*TCCS* [4]) that replaces the operators for internal transitions and for choice with the operators for internal choice and for purely external choice.[1] We have chosen TCCS for the sake of simplicity and for avoiding the well known congruence problem that

[1] These choice operators were originally introduced by Hoare, see e.g. [7], and their operational semantics was described in [11].

arises in presence of silent transitions and choice. All of our results can, however, be easily extended to CCS and similar calculi.

The rest of the paper is organized as follows. In Section 2, we briefly recall syntax and semantics of TCCS and the alternative characterizations of the observational semantics that will be used in later proofs. In Section 3, we prove that safe-testing is finer than readiness semantics and that it coincides with a fine tuning of the latter. In Section 4, we present complete equational characterizations of both safe-testing and readiness semantics. The final section contains some concluding remarks.

2. TCCS and its semantics

In this section, we briefly present syntax and semantics of TCCS (τ-less CCS [4, 5]). We let

- $\mathcal{N}$, ranged over by $a, b, \ldots$, be an infinite set of *names* and $\bar{\mathcal{N}} = \{\bar{a} \mid a \in \mathcal{N}\}$, ranged over by $\bar{a}, \bar{b}, \ldots$, be the set of *co-names*. $\mathcal{N}$ and $\bar{\mathcal{N}}$ are disjoint and are in bijection via the *complementation* function $(\bar{\cdot})$; we define: $\overline{(\bar{a})} = a$;
- $\mathcal{L} = \mathcal{N} \cup \bar{\mathcal{N}}$, ranged over by $\ell, \ell', \ldots$, be the set of *labels* (or *actions*); we shall use A, B and F to range over subsets of $\mathcal{L}$ and we define $\bar{A} = \{\bar{\ell} \mid \ell \in A\}$;
- $\mathcal{X}$, ranged over by $X, Y, \ldots$, be a countable set of *process variables*.

Definition 2.1 (*TCCS syntax*). The set of *TCCS terms* is generated by the grammar:

$$E ::= \mathbf{0} \mid \Omega \mid \ell.E \mid E[\,]F \mid E \oplus F \mid E|F \mid E\backslash A \mid E\{f\} \mid X \mid recX.E$$

where $f : \mathcal{L} \to \mathcal{L}$, is a *relabelling function* such that $\{\ell \mid f(\ell) \neq \ell\}$ is finite, $f(a) \in \mathcal{N}$ and $f(\bar{\ell}) = \overline{f(\ell)}$. We let $\mathcal{P}roc$, ranged over by P, Q, etc., denote the set of *closed* terms or *processes* (i.e. those terms where every occurrence of any process variable X lies within the scope of some $rec\,X._{-}$ operator).

For comments about the meaning of the operators above, we refer the reader to [4, 5, 11], here we simply explain basic notations. As usual, we shall write ℓ instead of $\ell.\mathbf{0}$, and write $E[E_1/X_1, \ldots, E_n/X_n]$ for the term obtained by simultaneously substituting each occurrence of X_i in E with E_i (while possibly renaming bound process variables). We write $\sum_{i\in\{1,\ldots,n\}} E_i$ as a shorthand of $E_1[\,]\cdots[\,]E_n$ (the order in which the operands E_i are arranged is irrelevant, as $[\,]$ is associative and commutative in every semantics considered in the paper); when $n = 0$, this term will by convention indicate $\mathbf{0}$. Similarly, for $n > 0$, we write $\sum_{i\in\{1,\ldots,n\}} E_i$ as a shorthand of $E_1 \oplus \cdots \oplus E_n$ (again, $\oplus$ is associative and commutative in every semantics considered in the paper).

The structural operational semantics of TCCS is defined via the two transition relations $\xrightarrow{\ell}$ (visible actions) and $\rightarrowtail$ (internal actions) defined in Table 1. As usual, we use $\Rightarrow$ or $\stackrel{\varepsilon}{\Rightarrow}$ to denote the reflexive and transitive closure of $\rightarrowtail$ and use $\stackrel{s}{\Rightarrow}$, with $s \in \mathcal{L}^+$, for $\Rightarrow \xrightarrow{\ell} \stackrel{s'}{\Rightarrow}$ when $s = \ell s'$. Moreover, we write $P \stackrel{s}{\Rightarrow}$ if there exists P' such that $P \stackrel{s}{\Rightarrow} P'$ ($P \xrightarrow{\ell}$ and $P \rightarrowtail$ will be used similarly). We say that a process is *stable* if

Table 1
TCCS SOS rules (symmetric variants of rules AR4, AR5, IR5, IR6 and IR7 omitted)

AR1 $\ell.P \xrightarrow{\ell} P$	
AR2 $\dfrac{P \xrightarrow{\ell} P'}{P\{f\} \xrightarrow{f(\ell)} P'\{f\}}$	AR3 $\dfrac{P \xrightarrow{\ell} P',\ \ell \notin A \cup \bar{A}}{P\backslash A \xrightarrow{\ell} P'\backslash A}$
AR4 $\dfrac{P \xrightarrow{\ell} P'}{P[]Q \xrightarrow{\ell} P'}$	AR5 $\dfrac{P \xrightarrow{\ell} P'}{P\|Q \xrightarrow{\ell} P'\|Q}$
IR1 $\Omega \rightarrowtail \Omega$	IR2 $recX.E \rightarrowtail E[recX.E/X]$
IR3 $\dfrac{P \rightarrowtail P'}{P\{f\} \rightarrowtail P'\{f\}}$	IR4 $\dfrac{P \rightarrowtail P'}{P\backslash A \rightarrowtail P'\backslash A}$
IR5 $P \oplus Q \rightarrowtail P$	IR6 $\dfrac{P \rightarrowtail P'}{P\,[]\,Q \rightarrowtail P'\,[]\,Q}$
IR7 $\dfrac{P \rightarrowtail P'}{P\|Q \rightarrowtail P'\|Q}$	IR8 $\dfrac{P \xrightarrow{\ell} P',\ Q \xrightarrow{\bar{\ell}} Q}{P\|Q \rightarrowtail P'\|Q'}$

it cannot perform internal actions. We will call *sort of* P the set of labels occurring in P (see, e.g., [8]) and *initial actions of* P the set $I(P) = \{\ell \in \mathscr{L} \mid P \stackrel{\ell}{\Rightarrow}\}$. In the actual proofs we will rely on the fact that, since we only consider finite relabelling operators, every TCCS process has a finite sort.

Now, we shall introduce the original *testing* scenario of [3, 5], the variant that leads to safe-must and its alternative characterizations.

Like in the original theory of testing [3, 5], we have that:

- *observers*, ranged over by $O, O', \ldots$, are processes capable of possibly performing an additional distinct "success" action $w \notin \mathscr{L}$;
- *computations* from $P|O$ are sequences of internal transitions

$$P \mid O\ (= P_0 \mid O_0) \rightarrowtail P_1 \mid O_1 \rightarrowtail \cdots$$

which are either infinite or such that there exists $k \geqslant 0$ with $P_k \mid O_k \not\rightarrowtail$.

Definition 2.2 (*Testing predicates*). Let P be a process and O be an observer.

(1) $P \underline{must}_M O$ if for each computation from $P|O$, say $P|O \rightarrowtail P_1|O_1 \rightarrowtail \cdots$, there is some $i \geqslant 0$ such that $O_i \xrightarrow{w}$.

(2) $P \underline{must}_{SM} O$ if for each computation from $P|O$, say $P|O \rightarrowtail P_1|O_1 \rightarrowtail \cdots$, there is some $i \geqslant 0$ such that $O_i \xrightarrow{w}$ and $P_i \downarrow$.

The first definition of successful computation given above is that of [3]. The second one, introduced in [1], considers successful only those computations that can report a success *strictly before* the observed process diverges. These notions lead to $\sqsubseteq_M$, the *must* preorder of [3, 5], and to $\sqsubseteq_{SM}$, the *safe-must* preorder of [1].

Definition 2.3 (*Testing preorders*). Let P and Q be processes and $X \in \{M, SM\}$ then

$$P \sqsubseteq_X Q \text{ if and only if for every observer } O\text{: } P \underline{must}_X O \text{ implies } Q \underline{must}_X O.$$

Given a preorder $\sqsubseteq_X$, the corresponding equivalence $\simeq_X$, is defined as $\simeq_X = \sqsubseteq_X \cap (\sqsubseteq_X)^{-1}$.

The preorders *must* and *safe-must* can be equipped with alternative characterizations that support simpler methods for proving (or disproving) that two processes are behaviourally related.

Definition 2.4. Let $s \in \mathscr{L}^*$, $B \subseteq_{\text{fin}} \mathscr{L}$ and $\mathscr{P}$ be a set of processes.

- The *convergence* predicate, $\downarrow s$, is defined inductively as follows:
  - $P \downarrow \varepsilon$ (or $P \downarrow$) if there is no infinite sequence of internal actions
    $$P \rightarrowtail P_1 \rightarrowtail P_2 \rightarrowtail \cdots;$$
  - $P \downarrow \ell s'$ if $P \downarrow \varepsilon$ and for each $P' : P \stackrel{\ell}{\Rightarrow} P'$ implies $P' \downarrow s'$.
    We write $P \uparrow s$ ($P \uparrow$) if $P \downarrow s$ ($P \downarrow$) does not hold.
- $(P \underline{after}\, s)$ is the set of processes $\{P' \mid P \stackrel{s}{\Rightarrow} P'\}$.
- $P \downarrow B$ means $P \downarrow \ell$ for each $\ell \in B$.
- $\mathscr{P} \downarrow B$ means $P \downarrow B$ for each $P \in \mathscr{P}$.
- $P \underline{accepts}_M B$ means that there exists $\ell \in B$ such that $P \stackrel{\ell}{\Rightarrow}$.
- $\mathscr{P} \underline{accepts}_M B$ means $P \underline{accepts}_M B$ for each $P \in \mathscr{P}$.
- $\mathscr{P} \underline{accepts}_{SM} B$ means $\mathscr{P} \downarrow B$ and $\mathscr{P} \underline{accepts}_M B$.

Definition 2.5 (*Alternative characterizations*). Let $X \in \{M, SM\}$. For processes P and Q, we write $P \ll_X Q$ if for each $s \in \mathscr{L}^*$ such that $P \downarrow s$, it holds that:
(a) $Q \downarrow s$, and
(b) for every $B \subseteq_{\text{fin}} \mathscr{L}$: $(P \underline{after}\, s) \underline{accepts}_X B$ implies $(Q \underline{after}\, s) \underline{accepts}_X B$.

The proof of the following results is reported in [1, 3, 5].

Theorem 2.6. *For all processes P and Q, $P \sqsubseteq_M Q$ if and only if $P \ll_M Q$.*

Theorem 2.7. *For all processes P and Q, $P \sqsubseteq_{SM} Q$ if and only if $P \ll_{SM} Q$.*

By taking advantage of the above alternative characterizations it is easy to prove that the must and the safe-must preorders are pre-congruences and that $\sqsubseteq_M$ is finer than $\sqsubseteq_{SM}$ (see, e.g., [1]).

We conclude the section by introducing the readiness semantics of TCCS processes as a literal translation of Olderog's definition (presented in Definition 4.4.1, p. 125 of [10]). Actually, our definition turns out to be slightly simpler because the TCCS operator for parallel composition does not make use of the sorts of the component processes, like in [10], and the previously mentioned "congruence problem" is absent.

Definition 2.8 (*Readiness*). The *readiness semantics* of a process P, $\mathscr{R}[\![P]\!]$, is defined as the union of three sets (which we label as (a)–(c) for ease of reference):

$$\mathscr{R}[\![P]\!] = \{(s,F) \mid \exists F' \colon (s,F') \in \Gamma(P),\ F' \subseteq F \subseteq succ(s,P)\} \tag{a}$$

$$\cup \{(s,X) \mid \exists s' \sqsubseteq s \colon (s',\uparrow) \in \Gamma(P),\ (X \subseteq \mathscr{L} \text{ or } X = \uparrow)\} \tag{b}$$

$$\cup \{(s,F) \mid \exists \ell \colon (s\ell,\uparrow) \in \Gamma(P),\ F \subseteq succ(s,P)\} \tag{c}$$

where

- $s' \sqsubseteq s$ if s' is a prefix of s;
- $succ(s,P) = \cup \{I(P') \mid P' \in (P \underline{after}\, s)\}$;
- $\Gamma(P) = \{(s, I(P')) \mid P \stackrel{s}{\Rightarrow} P'$ and P' is stable$\} \cup \{(s,\uparrow) \mid P \stackrel{s}{\Rightarrow} P'$ and $P' \uparrow\}$.

In the above definition, the set $succ(s,P)$ is the set of possible initial actions of P after trace s, i.e. visible actions that P can perform after s. Set F, where $(s,F) \in \Gamma(P)$, is a *ready set*, i.e. a set of communications in which the process is ready to engage when it has become stable after s. Trace s is a *divergent point* for P whenever $(s,\uparrow) \in \Gamma(P)$. The three sets, $(a-c)$ are the outcome of three closure operations:

(a) *acceptance closure*: any superset (composed of possible initial actions) of a ready set is a ready set as well;
(b) *chaotic closure*: divergent points add impredictability to all subsequent process behaviours (i.e. after a divergent point the effective process behaviour is ignored, indeed it is $X \subseteq \mathscr{L}$ rather than $X \subseteq succ(s,P)$), hence divergence is considered as catastrophic;
(c) *radiation closure*: divergence affects the ready sets one level up.

The *readiness preorder* is then defined as follows:

for all processes P and Q, $P \sqsubseteq_R Q$ if and only if $\mathscr{R}[\![Q]\!] \subseteq \mathscr{R}[\![P]\!]$.

The corresponding equivalence is called *readiness equivalence* and denoted by $\simeq_R$.[2]

3. A comparison of safe-must and readiness

To show that $\sqsubseteq_{SM}$ is finer than $\sqsubseteq_R$, we need a technical lemma, whose proof follows directly from the definitions.

Lemma 3.1. (1) *$P \uparrow s$ if and only if there is $s' \sqsubseteq s$ s.t. $(s',\uparrow) \in \Gamma(P)$.*
(2) *If $P \downarrow s$ and $(s,F) \in \mathscr{R}[\![P]\!]$ then $F \subseteq succ(s,P)$.*
(3) *If $P \sqsubseteq_{SM} Q$ and $P \downarrow s$ then $succ(s,Q) \subseteq succ(s,P)$.*

Theorem 3.2. *For all processes P and Q, $P \sqsubseteq_{SM} Q$ implies $P \sqsubseteq_R Q$.*

[2] Olderog directly introduces the equivalence without stepping on the preorder.

Proof. Suppose that $P \sqsubseteq_{SM} Q$ and that $(s,X) \in \mathscr{R}[\![Q]\!]$. We will show that $(s,X) \in \mathscr{R}[\![P]\!]$ as well. We distinguish two cases, namely $P \uparrow s$ and $P \downarrow s$.

If $P \uparrow s$, then there is $s' \sqsubseteq s$ s.t. $(s', \uparrow) \in \Gamma(P)$, by Lemma 3.1(1), hence $(s,X) \in \mathscr{R}[\![P]\!]$, by clause (b) of the definition of $\mathscr{R}[\![\cdot]\!]$.

Suppose now that $P \downarrow s$. From the alternative definition $\ll_{SM}$, we have that $Q \downarrow s$ too; thus, by Lemma 3.1(1), it must be the case that $X \neq \uparrow$, say $X = F$. Furthermore, by $P \sqsubseteq_{SM} Q$ and Lemma 3.1(2)–(3) we have that $F \subseteq succ(s,Q) \subseteq succ(s,P)$. We have now two subcases.

(a) For each ℓ, $P \downarrow s\ell$. From the alternative definition $\ll_{SM}$, we have that, for each ℓ, $Q \downarrow s\ell$ as well. Thus for no ℓ $(s\ell, \uparrow) \in \Gamma(Q)$, by Lemma 3.1(1). Since clauses (b) and (c) of Definition 2.8 do not apply for (s,F), by virtue of clause (a), there must exist Q' stable such that $Q \stackrel{s}{\Rightarrow} Q'$ and $I(Q') \subseteq F$. By contradiction, suppose now that $(s,F) \notin \mathscr{R}[\![P]\!]$. This fact implies that whenever $P \stackrel{s}{\Rightarrow} P_i$ there is some $a_i \in I(P_i) - F$ (by virtue of clause (a) and of $F \subseteq succ(s,P)$); moreover there are finitely many such a_i's, say n, because of sort-finiteness of P. Take now $F' = \{a_1, \ldots, a_n\}$: we have that $(P \underline{after}\, s)\, \underline{accepts}_{SM}\, F'$, while $(Q \underline{after}\, s)$ $\underline{a\not{c}cepts}_{SM}\, F'$, because $Q \stackrel{s}{\Rightarrow} Q'$ and $I(Q') \cap F' = \emptyset$. But this contradicts $P \sqsubseteq_{SM} Q$.

(b) There is ℓ such that $P \uparrow s\ell$. Since $P \downarrow s$, this implies that there is P' s.t. $P \stackrel{s\ell}{\Rightarrow} P'$ and $P' \uparrow$, i.e. $(s\ell, \uparrow) \in \Gamma(P)$. Since $F \subseteq succ(s,P)$, by virtue of clause (c) of Definition 2.8 we get $(s,F) \in \mathscr{R}[\![P]\!]$. □

To show that the converse of the theorem above does not hold, we exhibit a counterexample.

Counterexample 3.3. Take the processes $P = a.\Omega[\,]b$ and $Q = (a.\Omega[\,]b) \oplus \mathbf{0}$. We have $\Gamma(P) = \{(\varepsilon, \{a,b\}), (a, \uparrow), (b, \emptyset)\}$ and $\Gamma(Q) = \{(\varepsilon, \{a,b\}), (a, \uparrow), (b, \emptyset), (\varepsilon, \emptyset)\}$. Hence

$$\mathscr{R}[\![P]\!] = \{(\varepsilon, \{a,b\}), (a, \uparrow), (b, \emptyset), (\varepsilon, \emptyset), (\varepsilon, \{a\}), (\varepsilon, \{b\})\}$$
$$\cup \{(as, \uparrow) | s \in \mathscr{L}^*\} \cup \{(as, F) | s \in \mathscr{L}^*, F \subseteq \mathscr{L}\} = \mathscr{R}[\![Q]\!]$$

that, in particular, implies that $P \sqsubseteq_R Q$. However, taking the observer $O = \bar{b}.w$, we have $P\, \underline{must}_{SM}\, O$, but $Q\, \underline{m\not{u}st}_{SM}\, O$, thus $P \not\sqsubseteq_{SM} Q$.

Note that both Theorem 3.2 and the counterexample above can be established for the equivalences too. Hence, we have that $\simeq_{SM}$ is finer than $\simeq_R$. The difference between Olderog's semantics and our safe-must is indeed very small, and is due to set (c) of $\mathscr{R}[\![\,]\!]\cdot$; a mild restriction of this set leads to safe-must.

Definition 3.4 (*Readiness revisited*). The *revisited readiness semantics* of a process P, $\mathscr{S}[\![P]\!]$, is defined by changing set (c) of Definition 2.8 into set (c'):

$$\{(s,F) | F \subseteq succ(s,P) \text{ and}$$

$$\exists F'\colon\ (s,F')\in\Gamma(P),\ F'-F\neq\emptyset \text{ and } \forall \ell\in F'-F\colon\ (s\ell,\uparrow)\in\Gamma(P)\},\qquad (c')$$

where $\Gamma(P)$ and $succ(s,P)$ are as in Definition 2.8.

It is possible to give a simpler definition of $\mathscr{S}[\![\cdot]\!]$ by unifying clauses (a) and (c′), but the one we chose highlights precisely the difference from Olderog's. In passing, note that ignoring (c) would lead to a semantics which is fully abstract for must testing. Of course, Lemma 3.1 (in particular, case 2), still holds when replacing $\mathscr{R}[\![\cdot]\!]$ with $\mathscr{S}[\![\cdot]\!]$.

Theorem 3.5. *$P \sqsubseteq_{\approx SM} Q$ if and only if $\mathscr{S}[\![Q]\!]\subseteq\mathscr{S}[\![P]\!]$.*

Proof. The proof that $P\sqsubseteq_{\approx SM} Q$ implies $\mathscr{S}[\![Q]\!]\subseteq\mathscr{S}[\![P]\!]$ has the same structure as that of Theorem 3.2, with $\mathscr{R}[\![\cdot]\!]$ replaced by $\mathscr{S}[\![\cdot]\!]$ and (c) by (c′), but the case when $P\downarrow s$ is dealt with differently; this we do below.

Suppose by contradiction that $(s,F)\notin\mathscr{S}[\![P]\!]$. This implies that whenever $P\stackrel{s}{\Rightarrow}P_i$ there is some $a_i\in I(P_i)-F$ s.t. $P\downarrow sa_i$: otherwise, we could deduce that $(s,F)\in\mathscr{S}[\![P]\!]$ by virtue of $F\subseteq succ(s,P)$ and of clauses (a) or (c′). Due to sort-finiteness, there are finitely many a_i's, say $F'=\{a_1,\ldots,a_n\}$. By construction, $F\cap F'=\emptyset$ and $(P\ \underline{after}\ s)\ \underline{accepts}_{SM}\ F'$. On the other hand, $(s,F)\in\mathscr{S}[\![Q]\!]$ implies that there exists Q' stable such that $Q\stackrel{s}{\Rightarrow}Q'$ and for each $\ell\in I(Q')-F$: $(s\ell,\uparrow)\in\Gamma(Q)$ (union of clauses (a) and (c') of the definition of $\mathscr{S}[\![\cdot]\!]$); hence, from $F\cap F'=\emptyset$, we deduce that for each $\ell\in I(Q')\cap F'$ we have $Q'\uparrow\ell$. This allows us to deduce the contradiction $(Q\ \underline{after}\ s)\ \underline{\not accepts}_{SM}\ F'$: indeed, either $I(Q')\cap F'=\emptyset$ or there is $\ell\in I(Q')\cap F'$ such that $\overline{Q'\uparrow\ell}$.

The proof of the converse ($\mathscr{S}[\![Q]\!]\subseteq\mathscr{S}[\![P]\!]$ implies $P\sqsubseteq_{\approx SM} Q$), is an easy consequence of the following fact, whose simple proof is omitted. Suppose that $P\downarrow s$; then $(P\ \underline{after}\ s)\ \underline{accepts}_{SM}\ B$ if and only if the following properties hold:

- $P\downarrow s\ell$, for each $\ell\in B$,
- $F\cap B\neq\emptyset$, for each $(s,F)\in\mathscr{S}[\![P]\!]$. □

4. Axiomatizations

In this section we shall present two complete axiomatizations, one for $\sqsubseteq_{\approx SM}$, the other for $\sqsubseteq_{\approx R}$ (they will also give complete axiomatizations for $=_{SM}$ and $=_R$, respectively). Each of the two axiomatizations will be obtained by adding a single new law to an existing axiomatization for the original must preorder, $\sqsubseteq_{\approx M}$. The precise axiomatization chosen for $\sqsubseteq_{\approx M}$ is irrelevant. Let $\mathscr{M}$ be any such axiomatization (e.g., the axiomatization presented in [5]): we shall write $P\sqsubseteq_{\mathscr{M}} Q$ (resp. $P=_{\mathscr{M}} Q$) if $P\sqsubseteq Q$ (resp. both $P\sqsubseteq Q$ and $Q\sqsubseteq P$) can be proven within $\mathscr{M}$.

4.1. Safe-testing

The axiomatization for safe-testing is obtained by adding the law

$$\ell.\Omega\sqsubseteq\ell.\Omega\oplus\mathbf{0}\qquad (S)$$

to the complete axiomatization $\mathscr{M}$ of must testing. Below, we prove this result while confining ourselves to finite processes, but we do not foresee much difficulty in extending the result to general processes by relying on a (non-effective) ω-induction rule, like in [3, 5]. In the sequel, we shall write $P \sqsubseteq_{SM} Q$ (resp. $P =_{SM} Q$) if $P \sqsubseteq Q$ (resp. both $P \sqsubseteq Q$ and $Q \sqsubseteq P$) can be proven within $\mathscr{M} \cup \{\mathtt{S}\}$.

The key to the proof is showing that must and safe-must coincide over standard forms for processes, saturated with respect to left-to-right applications of law $\ell.\Omega = \ell.\Omega \oplus \mathbf{0}$, which is derived from S and from $P \oplus Q \sqsubseteq P$ (the latter holds for all the preorders we consider).

Definition 4.1 (*Safe sum-forms*).

- *Sum-forms* are inductively defined as follows:
  - Ω is a sum-form;
  - $\sum_{A\in\mathscr{A}} \sum_{\ell\in A} \ell.P_\ell$ is a sum-form if P_ℓ is a sum-form for each $\ell \in \cup\{A : A \in \mathscr{A}\}$ and $\mathscr{A} \neq \emptyset$.
- A sum-form S is *safe* if whenever $S = \sum_{A\in\mathscr{A}} \sum_{\ell\in A} \ell.P_\ell$ then
  (a) if $P_{\ell_0} \Rightarrow \Omega$, for some $\ell_0 \in A$ with $A \in \mathscr{A}$, then $A - \{l_0\} \in \mathscr{A}$
  (b) each P_ℓ is safe.

Note that the terms P_ℓ only depend on the label ℓ and that, by definition, Ω is a safe sum-form. Also note that $\sum_{A\in\mathscr{A}} \sum_{\ell\in A} \ell.P_\ell \Rightarrow \sum_{\ell\in A} \ell.P_\ell$, for each $A \in \mathscr{A}$. In the proof of the following lemma, we shall use the notation "$P \stackrel{s}{\Rightarrow} P'$" as a shorthand of "$P = P'$" if $s = \varepsilon$ or "$P \stackrel{s'}{\Rightarrow} \stackrel{\ell}{\rightarrow} P'$" if $s = s'\ell$.

Lemma 4.2. *Let S be a safe sum-form and suppose that $S \downarrow s$ and $S \uparrow s\ell_0$. Then it holds that*:

$$(S \underline{\ after\ } s)\underline{accepts}_M B \text{ if and only if } (S \underline{\ after\ } s)\underline{accepts}_M B - \{\ell_0\}$$

Proof. The 'if' direction is trivial. Suppose now that $(S \underline{after}\, s)\, \underline{accepts}_M B$, we want to show that $(S \underline{after}\, s)\, \underline{accepts}_M B - \{\ell_0\}$. Let $U \in (S \underline{after}\, s)$, we must prove that $I(U) \cap (B - \{\ell_0\}) \neq \emptyset$. Since by hypothesis it must be $I(U) \cap B \neq \emptyset$, it will be sufficient to show that $I(U) \cap B \neq \{\ell_0\}$. By contradiction, assume that $I(U) \cap B = \{\ell_0\}$. Since S is a sum-form, we can easily prove (by induction on s) that there is a *unique* T such that

$$S \stackrel{s}{\Rightarrow} T.$$

T is a safe sum-form (since S is). Furthermore, since $T \Rightarrow U$ and $I(U) \neq \emptyset$, it is $T \neq \Omega$, say $T = \sum_{A\in\mathscr{A}} \sum_{\ell\in A} \ell.P_\ell$. Now, since $I(U) \cap B = \{\ell_0\}$, we deduce that there is $A \in \mathscr{A}$ such that $A \cap B = \{l_0\}$. Since $S \downarrow s$, $S \uparrow s\ell_0$ and T is unique, we deduce that $T \uparrow \ell_0$, hence $P_{\ell_0} \Rightarrow \Omega$. But T is safe, thus we get that $A - \{\ell_0\} \in \mathscr{A}$. Therefore we get $T \Rightarrow \sum_{\ell\in A-\{\ell_0\}} \ell.P_\ell \stackrel{\text{def}}{=} U'$, with $I(U') \cap B = A - \{\ell_0\} \cap B = \emptyset$: but this contradicts $(S \underline{after}\, s)\, \underline{accepts}_M B$. □

Proposition 4.3. *Let S be a safe sum-form. Then, for any Q, $S \sqsubseteq_M Q$ if and only if $S \sqsubseteq_{SM} Q$.*

Proof. One direction is trivial, as $\sqsubseteq_M$ is finer than $\sqsubseteq_{SM}$. Conversely, suppose that $S \sqsubseteq_{SM} Q$, that $S \downarrow s$ and that $(S \underline{after}\, s)\, \underline{accepts}_M B$ for any s and B: we show that $Q \downarrow s$ and that $(Q \underline{after}\, s)\, \underline{accepts}_M B$, thus proving that $S \sqsubseteq_M Q$.

$Q \downarrow s$ trivially follows from the definitions of the alternative characterizations. Next, define $B' \stackrel{\text{def}}{=} \{\ell \in B : S \downarrow s\ell\}$. Applying (repeatedly) Lemma 4.2, since B and thus $B - B'$ are finite, we obtain $(S \underline{after}\, s)\, \underline{accepts}_M B'$. Since $S \downarrow s\ell$ for each $\ell \in B'$, we get by definition also that $(S \underline{after}\, s)\, \underline{accepts}_{SM} B'$. Since $S \sqsubseteq_{SM} Q$ and $S \downarrow s$, we deduce that $(Q \underline{after}\, s)\, \underline{accepts}_{SM} B'$. But this implies $(Q \underline{after}\, s)\, \underline{accepts}_M B'$, since $\underline{accepts}_{SM}$ is stronger than $\underline{accepts}_M$. Finally, since $B \supseteq B'$, we get that $(Q \underline{after}\, s)\, \underline{accepts}_M B$, the wanted claim.

Theorem 4.4 (soundness and completeness for safe-must). *$P \sqsubseteq_{SM} Q$ if and only if $P \sqsubseteq_S Q$.*

Proof. For proving soundness it is sufficient to check validity of law S, which is immediate. Let us examine completeness. From [5], we know that there exists a sum-form S such that $P =_M S$. Then, applying repeatedly law $\ell.\Omega = \ell.\Omega \oplus \mathbf{0}$ and law $(\ell.\Omega \oplus \mathbf{0})[\,]Q =_M (\ell.\Omega[\,]Q) \oplus Q$, we can get out of S a safe sum-form S' such that $S =_{SM} S'$. By soundness $S' \sqsubseteq_{SM} Q$, hence, by Proposition 4.3, $S' \sqsubseteq_M Q$. From completeness of must preorder, we get that $S' \sqsubseteq_M Q$. This allow us to infer the wanted $P \sqsubseteq_{SM} Q$. □

Obviously, $\mathcal{M} \cup \{\mathrm{S}\}$ also give a complete axiomatization for $\simeq_{SM}$: to prove that $P \simeq_{SM} Q$, it is enough to prove both $P \sqsubseteq_{SM} Q$ and $Q \sqsubseteq_{SM} P$.

4.2. Readiness semantics

The axiomatization for readiness semantics is obtained by adding the law

$$\ell.\Omega[\,]P \sqsubseteq (\ell.\Omega[\,]P) \oplus \mathbf{0} \qquad (\mathrm{R})$$

to the complete axiomatization $\mathcal{M}$ of must testing. Below, we confine ourselves to finite processes (again, we do not foresee much difficulty in extending the result to general processes by relying on an ω-induction rule). In the sequel, we shall write $P \sqsubseteq_R Q$ (resp. $P =_R Q$) if $P \sqsubseteq Q$ (resp. both $P \sqsubseteq Q$ and $Q \sqsubseteq P$) can be proven within $\mathcal{M} \cup \{\mathrm{R}\}$.

Again, the key step is showing that must and readiness semantics coincide over normal forms saturated with respect to left-to-right applications of the law $\ell.\Omega[\,]P = (\ell.\Omega[\,]P) \oplus \mathbf{0}$, which trivially follows from R and from $P \oplus Q \sqsubseteq P$. In the definition below, recall that a summation $\sum$ over an empty set of indices denotes $\mathbf{0}$ by convention.

Definition 4.5 (*Ready sum-forms*). A sum-form S is *ready* if whenever $S = \sum_{A\in\mathscr{A}} \sum_{\ell\in A} \ell.P_\ell$ then
(a) if $P_{\ell_0} \Rightarrow \Omega$, for some $\ell_0 \in A$ with $A \in \mathscr{A}$, then $\emptyset \in \mathscr{A}$
(b) each P_ℓ is ready.

Note that, by definition, Ω is a ready sum-form. The proof of the following lemma follows directly from the definitions.

Lemma 4.6. *Let S be a ready sum-form and suppose that $S \downarrow s$. Then*:
(1) *If $S \uparrow s\ell$, for some ℓ, then for no B it holds that $(S \underline{after}\, s)\, \underline{accepts}_M\, B$.*
(2) *Suppose that $S \downarrow s\ell$, for each ℓ. Then $(S \underline{after}\, s)\, \underline{accepts}_M\, B$ if and only if for each $(s,F) \in \mathscr{R}[\![P]\!]$ it holds that $F \cap B \neq \emptyset$.*

Proposition 4.7. *Let S and R be a ready sum-forms. Then $S \sqsubseteq_M R$ if and only if $S \sqsubseteq_R R$.*

Proof. One direction is trivial, as $\sqsubseteq_M$ is finer than $\sqsubseteq_{SM}$ that is finer than $\sqsubseteq_R$. Conversely, suppose that $S \sqsubseteq_R R$, that $S \downarrow s$ and that, for any s and B, $(S \underline{after}\, s)\, \underline{accepts}_M\, B$: we show that $R \downarrow s$ and that $(R \underline{after}\, s)\, \underline{accepts}_M\, B$, thus proving that $S \sqsubseteq_M R$.

$R \downarrow s$ trivially follows from Lemma 3.1(1). Next, from Lemma 4.6(1) and $(S \underline{after}\, s)\, \underline{accepts}_M\, B$, we deduce that for each ℓ it is $S \downarrow s\ell$, hence $R \downarrow s\ell$. From Lemma 4.6(2) we get that for each $(s,F) \in \mathscr{R}[\![S]\!]$ it holds that $F \cap B \neq \emptyset$. Since $\mathscr{R}[\![R]\!] \subseteq \mathscr{R}[\![S]\!]$, we have that the same holds for R, hence, again for the same lemma, $(R \underline{after}\, s)\, \underline{accepts}_M\, B$, the wanted claim. □

Theorem 4.8 (Soundness and completeness for readiness semantics). *$P \sqsubseteq_R Q$ if and only if $P \sqsubseteq_R Q$.*

Proof. For proving soundness it is sufficient to check validity of law (R), which is immediate. Let us examine completeness. From [5], we know that there are sum-forms S and R such that $P =_M S$ and $Q =_M R$. Now, applying repeatedly law $\ell.\Omega[\,]P = (\ell.\Omega[\,]P) \oplus \mathbf{0}$, we can get out of S and R two ready sum-forms S' and R' such that $S =_R S'$ and $R =_R R'$. By soundness $S' \sqsubseteq_R R'$, hence, by Proposition 4.3, $S' \sqsubseteq_M R'$. From completeness for must, we get that $S' \sqsubseteq_M R'$. This allows us to infer the wanted $P \sqsubseteq_R Q$. □

Finally, note that $\mathscr{M} \cup \{\mathrm{R}\}$ also gives a complete axiomatization for $\simeq_R$.

5. Conclusions

We have axiomatized safe-testing, a variant of must testing that imposes stronger requirements for considering computations as successful. We have proven that safe-

testing is finer than Olderog's readiness semantics and coincides with a fine tuning of the latter. We have also exhibited an axiomatization of readiness semantics.

The results presented in the paper for TCCS can be easily extended to CCS and similar calculi. They can also be extended to process algebras with value-passing, such as the TCCS version considered in [6]. A value-passing process can in general perform an infinite number of actions, thus it is not sort-finite; for instance, process $c?x.\mathbf{0}$, that inputs a value along channel c and terminates, has an infinite number of derivations $c?x.\mathbf{0} \stackrel{c?v}{\rightarrow} \mathbf{0}$, one for each element v of an infinite set of values. However, all of our results can be generalized, because they rely on finiteness of the set of communication channels that processes can use, not on sort-finiteness.

Acknowledgements

We are grateful to E.-R. Olderog for e-mail discussions on safe-testing and readiness semantics. An anonymous referee provided helpful suggestions for improving the paper.

References

[1] M. Boreale, R. De Nicola, R. Pugliese, Basic observables for processes, Inform. and Comput. 149 (1) (1999) 77–98.
[2] E. Brinksma, A. Rensink, W. Vogler, Fair testing, in: I. Lee, S.A. Smolka (Eds.), Proc. CONCUR'95, Lecture Notes in Computer Science, vol. 962, Springer, Berlin, 1995, pp. 313–327.
[3] R. De Nicola, M. Hennessy, Testing equivalence for processes, Theoret. Comput. Sci. 34 (1984) 83–133.
[4] R. De Nicola, M. Hennessy, CCS without τ's, in: H. Ehrig, et al., (Eds.), Proc. TAPSOFT'87, Lecture Notes in Computer Science, vol. 249, Springer, Berlin, 1987, pp. 138–152.
[5] M. Hennessy, Algebraic Theory of Processes, MIT Press, Cambridge, MA, 1988.
[6] M.C.B. Hennessy, A. Ingolfsdottir, A theory of communicating processes with value-passing, Inform. and Comput. 107 (2) (1993) 202–236.
[7] C.A.R. Hoare, Communicating Sequential Processes, Prentice-Hall, Englewood Cliffs, NJ, 1985.
[8] R. Milner, Communication and Concurrency, Prentice-Hall, Englewood Cliffs, NJ, 1989.
[9] V. Natarajan, R. Cleaveland, Divergence and fair testing, in: Z. Fulop, F. Gécseg (Eds.), Proc. ICALP'95, Lecture Notes in Computer Science, vol. 944, Springer, Berlin, 1995, pp. 648–659.
[10] E.-R. Olderog, Nets, Terms and Formulas, Cambridge Tracts in Theoretical Computers Science, vol. 23, Cambridge University Press, Cambridge, 1991.
[11] E.-R. Olderog, C.A.R. Hoare, Specification-oriented semantics for communicating processes, Acta Inform. 23 (1986) 9–66.