Math. Struct. in Comp. Science (2009), *vol.* 19, *pp.* 959–1027. © Cambridge University Press 2009
doi:10.1017/S0960129509990077 First published online 4 September 2009

Algebra and logic for resource-based systems modelling

MATTHEW COLLINSON[†] and DAVID PYM[†‡]

[†]*Hewlett-Packard Laboratories, Bristol, BS34 8QZ, United Kingdom*
[‡]*University of Bath, Bath, BA2 7AY, United Kingdom*

Received 12 December 2007; revised 1 June 2009

Mathematical modelling is one of the fundamental tools of science and engineering. Very often, models are required to be executable, as a simulation, on a computer. In this paper, we present some contributions to the process-theoretic and logical foundations of discrete-event modelling with resources and processes. We present a process calculus with an explicit representation of resources in which processes and resources co-evolve. The calculus is closely connected to a logic that may be used as a specification language for properties of models. The logic is strong enough to allow requirements that a system has a certain structure: for example, that it is a parallel composite of subsystems. This work consolidates, extends and improves upon aspects of earlier work of ours in this area. An extended example, consisting of a semantics for a simple parallel programming language, indicates a connection with separating logics for concurrency.

1. Introduction

Mathematical modelling and simulation are fundamental tools of science and engineering. They are important in almost all fields, at many scales and at many levels of complexity. This paper deals with the mathematical and logical foundations of discrete-event modelling.

Modelling is the process of making a precise description, a *model*, of a system in order that its properties may be subjected to a rigorous analysis. The precise form of the model, the analysis it is subjected to and even the modelling process itself depend upon the object of study. However, some general observations are in order to put this paper in context. Any model should be *sound* in the sense that all parts somehow represent aspects of the system being modelled. On the other hand, a model need not be *complete* in order for it to be useful, since it does not have to represent every aspect of the system being described. Thus it is important to distinguish between the model and the underlying system that the model represents. Very often this introduces feedback into the modelling process, in which a hierarchy of successively refined models is created.

One kind of model that frequently arises is the *discrete-event* model. In such models, the (model of the) system evolves in discrete jumps. In traditional applied mathematics, such systems are often described by families of difference equations that describe how the system changes locally in time from one instant to the next. From these equations an evolution (or flow) operator is produced that completely describes the behaviour of the system. This calculation method is undoubtedly very powerful, but in practice, it

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

can be difficult to formulate the equations in a soluble form. This is often the case when the system is complex: for example, with many mutually dependent, heterogeneous components, evolving concurrently in different ways and on different time-scales. In such situations, when calculation is difficult, infeasible or cannot be carried out within a given time, it can be particularly useful to produce a computational model of the system. In practice this is done with a whole host of programming languages and tools. There are even languages specifically designed for such tasks, with perhaps the best-known simulation language being Simula (Dahl *et al.* 1970). Most of the time the semantics of such languages are not well understood. Recall, however, the soundness criterion on models. There is a need for simulation languages that rest upon rigorous foundations in order that no spurious trajectories are introduced inadvertently into simulations.

In this paper, we use Demos2k (Birtwistle and Tofts 2001a; 2001b; The Demos 2000 Team 2002) as an important example of such a language. Demos2k is a descendant of the original Demos tool (Birtwistle 1979), which itself is a descendant of Simula. From now on, all specific references we make to the workings of Demos should be taken to refer to the later Demos2k. Demos is a discrete-event modelling tool used to describe the concurrent co-evolution of many *entities*, together with the *resources* they use. It is closely related to languages for concurrent and distributed programming (Ben-Ari 1990). The soundness of Demos2k as a modelling tool is encapsulated in the statement that it is *semantically justified*: there is a precise mathematical description of the structure and evolution of every model written in the language. Alternative modelling tools that use languages influenced by the theory of semantics include the Concurrency Workbench (Cleaveland *et al.* 1993), the Mobility Workbench (Victor and Moller 1994) and PRISM (Hinton *et al.* 2006). In addition, there is a well-developed modelling paradigm in which systems of interest are characterised in terms of their environment (typically represented as collections of stochastic events), the spatial or logical distribution of the system, the resources present in the system and the processes that the system executes. Further discussion of this paradigm is beyond the scope of this paper, but the analysis we present here provides direct support for the last two aspects mentioned. Demos conforms much more closely with this paradigm than do the alternative tools mentioned above.

The area of semantics most closely connected to this kind of work is known as *process calculus* (or process algebra). A process calculus can be thought of as a precise mathematical language for describing concurrently evolving entities called *processes*. Indeed, they can fruitfully be thought of as idealised simulation languages (of a certain kind). This point of view has been expounded by others in the past, and a significant body of work has been built up in pursuing it. The paper Birtwistle *et al.* (1993), for example, is a good introduction, whilst Tofts (2006) provides an appraisal of the methodology, including an account of its scope and suggestions of areas and problems to which it may be expected to make further contributions.

The process calculi that we shall develop in this paper are strongly influenced by Milners' Synchronous Calculus of Communicating Processes SCCS (Milner 1983). This followed an earlier development, CCS, which was asynchronous (Milner 1980; 1989). Other process calculi emerged around the same time from other researchers, and there have been many developments since, but for the most part these will not concern us here. Baeten (2005) provides a survey of the history of process calculi.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

A good process calculus usually has several distinguishing features. To begin with, processes should be constructed formally from a well-defined collection of atomic *actions* and a small number of process *constructors*. Models of systems are assembled from sub-models by means of the constructors. The meaning of every process should be given by a *structural operational semantics* (Plotkin 2004), with constructors having a natural, intuitive reading. The operational semantics generates a *transition structure* (or system) that describes the flow of processes. An algebraic theory of process equality called *(bi)simulation* is used to identify processes with the same behaviour. In addition, it is usually necessary (for entirely practical reasons) to have a second language that makes logical assertions about properties of processes. Thus the process calculus presents not only a precise description of the evolution of processes but also a method for specifying and verifying process properties. Certain forms of process are known to give rise to terminating algorithms for constructing transition structures, and for model-checking processes against specifications. Automated tools are then often provided in support. When all of these features are present, the process calculus may be seen to be an integrated environment for both the synthesis and analysis of models.

There are, however, some difficulties associated with using existing process calculi as a foundation for modelling and simulation of the kind we have described, although it can be done (Birtwistle *et al.* 1993). These difficulties arise from there being no *direct* representation of resources, which must therefore be represented via an encoding. This has two consequences: first, there is a lack of a clear conceptual analysis of the notion of a resource, a significant burden for the modeller who must track important quantitative information conveyed by the resource; and, second, keeping track of the evolution of resources becomes a heavy burden when computing the evolution of a process.

The process algebra **SCRP**, Synchronous Calculus of Resource Processes, introduced in Pym and Tofts (2006; 2007) and Collinson *et al.* (2007), provides the beginnings of an approach to addressing these issues. In **SCRP**, resources are taken to be first-class citizens along with processes. That is, a model consists of a complex process together with some resources. The notion of resources used is closely related to the resource-semantics of the **BI**-family of logics (O'Hearn and Pym 1999; Pym 1999; Pym *et al.* 2004; Pym 2002), which have enjoyed a good deal of attention in recent years, particularly in the guise of the program logic known as Separation Logic (Ishtiaq and O'Hearn 2001; Reynolds 2002; O'Hearn 2007). Such logics have variants of standard logical connectives that are often useful for internalising statements about resource usage. The modelling approach that **SCRP** is intended to support is reflected in, and begins with, its treatment of resources. Specifically, it is hypothesised that the following properties of resources are basic:

— a basic collection of resource elements, including a zero element;
— a notion of combination of resource elements; and
— a notion of comparison of resource elements.

These properties are captured mathematically as a preordered, (initially) commutative monoid $(\mathbf{R}, \circ, e, \sqsubseteq)$ satisfying various algebraic laws, including a functoriality condition for the product relative to the order.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

The basic judgement in **SCRP** is the evolution of a process relative to a collection of resources,

$$R, E \xrightarrow{a} R', E',$$

where the resource $R' = \mu(a, R)$ is determined by a *modification function* μ defined on pairs of actions and resources. The basic judgement for action prefix then has the form

$$\frac{}{R, a : E \xrightarrow{a} \mu(a, R), E}$$

As well as straightforward non-deterministic sum, **SCRP** admits a synchronous concurrent product (recall the generality of the synchronous product (Milner 1983; de Simone 1985) which requires the monoidal product on resources – roughly

$$\frac{R, E \xrightarrow{a} R', E' \quad S, F \xrightarrow{b} S', F'}{R \circ S, E \times F \xrightarrow{ab} R' \circ S', E' \times F'}$$

There is also a hiding operator – roughly,

$$\frac{R \circ S, E \xrightarrow{a} R' \circ S', E'}{R, \nu S.E \xrightarrow{\nu S.a} R', \nu S'.E'}$$

in which part of the initial resource is bound locally to the process. This construct allows, among other things, **SCRP** to recover concepts that are expressible using the restriction combinator of SCCS.

SCRP's use of the same structure for resources as used in bunched logics suggests the possibility of a logic, in the style of Hennessy–Milner logic, characterising the combinatorial structure of the calculus. The semantic judgement of this logic, called **MBI**, takes the form

$$R, E \models \phi,$$

which is read as 'the property ϕ holds for the process E relative to resources R' or 'ϕ is true for the system R, E'. Such a logic can be thought of as providing a language **MBI** for specifying and verifying systems expressed, using **SCRP**, as assemblies of resources and processes. One valuable and useful consequence of this set-up is that the **MBI**-language leads to a logical characterisation of the synchronous product – roughly, we get

$$R, E \models \phi_1 * \phi_2$$

if and only if there exist R_1 and R_2 such that $R_1 \circ R_2 = R$, and E_1 and E_2 such that $E_1 \times E_2 \sim E$, where $\sim$ is an appropriate notion of bisimulation, such that

$$R_1, E_1 \models \phi_1 \quad \text{and} \quad R_2, E_2 \models \phi_2.$$

The hiding construct is characterised in a similar way using a quantifier (see Section 3.5). The presence of these decompositions emphasises the value of the two-language (algebraic and logical) approach to process calculus and modelling.

The process calculus **SCRP** and its logic **MBI** were introduced in the three papers Pym and Tofts (2006; 2007) and Collinson *et al.* (2007), the last of these correcting an error in the first two. The intention of these papers was to establish the core ideas of the calculi

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

and to demonstrate their practical effectiveness as a foundation for systems modelling in the spirit of Demos. Those papers did not, however, address a number of important theoretical issues relating to the metatheories of the calculi and the structures of the spaces over which they are defined. In this paper, we give a thorough investigation of these issues and show that the calculi can be significantly improved by making a number of small changes to the set-up.

This paper presents further developments, and a consolidation, of the ideas introduced in Pym and Tofts (2006; 2007) and Collinson *et al.* (2007). We present a new calculus **SCRPr** and logic with several important technical refinements that lead to better theoretical properties. The first refinement is to pick out a new kind of (bi)simulation relation, written $\sim$, which is a congruence. Certain identities for $\sim$ are seen to depend critically upon structural properties of the operational semantics. The simulation leads to a logic of system properties and part of a suitable Hennessy–Milner theorem. The third contribution is to introduce a proof system for (the propositional fragment of) the modal logic **MBI**. This is particularly important as the general model-checking problem for **MBI** is hard. The combination of substructural connectives means that the soundness result for the logic is non-trivial: indeed, it depends upon the Hennessy–Milner theorem. We study the way in which additional structure on resources is connected to the fundamental design of such process and logical calculi. In particular, we set up an intuitionistic version of the logic on an ordered state space. We study asynchrony and value passing in **SCRP**-like calculi. Finally, we sketch a semantics of a simple programming language with heap-manipulating commands.

Section 2 of this paper sets up the process calculus and its simulation relations, and develops the algebraic theory. Section 3 gives an account of the logical calculi, the associated Hennessy–Milner theorem and the soundness result. Section 4 investigates calculi in the presence of an ordered structure on resources and an intuitionistic logic. Section 5 gives extensions of the calculus to treat asynchrony and value passing, and sketches the development of a parallel programming language with variable assignment. Section 6 discusses work in progress on extending and applying the calculus.

Finally, the reader should be aware that certain words used in this paper will have more than one technical meaning: for example, the words model and simulation. This unavoidable clash comes about because we are drawing upon the traditions of mathematical logic and theoretical computer science as well as those of applied mathematics. We hope that the reader will not have any difficulty in understanding what is meant in each context.

2. A Synchronous Calculus of Resources and Processes

The process algebra **SCRP** was sketched, along with its associated logic (**MBI**) and various properties, in Pym and Tofts (2006; 2007) and Collinson *et al.* (2007). In this section, we give a refined presentation of a family of systems, collectively known as **SCRP**, along with their key technical properties. We make (*ad hoc*) naming distinctions between the **SCRP** variants as necessary. In particular, we present a calculus with theoretical properties that are significantly improved relative to those of the system that have been sketched

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

previously. We also make a more detailed study of (bi)simulation relations and their corresponding algebraic theories. Indeed, we draw attention to a notion of (bi)simulation that was not presented in the earlier work and is essential for the logical work that follows.

2.1. *The process calculus*

We now present a process calculus **SCRPr** that is a better-behaved, though less general, variant of the calculus **SCRP** presented in Pym and Tofts (2006; 2007) and Collinson *et al.* (2007). The set-up of these calculi assumes the provision of certain additional data pertaining to some semantic structure $(\mathsf{Act}, \mathbf{R}, \mu, \nu)$ over which we are working. Thus we should properly refer to the calculus as $(\mathsf{Act}, \mathbf{R}, \mu, \nu)$-**SCRPr**. In this paper, however, we suppress the prefix as, at every stage, we work with a fixed such structure.

We assume a commutative monoid, Act, of *actions*. Just as in standard process algebra, these actions correspond to the events of a system. We reserve the letters a, b, c for actions. Composition is written by juxtaposition and the unit action is written 1. We do not, for now, need to assume that this monoid is generated from a collection of atomic actions (usually called particles). Nor do we need any assumptions about the cardinality of Act.

In this paper we shall often work with partial functions. We use the standard notations $R\downarrow$ and $R\uparrow$ to mean that an expression R is defined or undefined, respectively. We also make use of Kleene equality between expressions: the left-hand side of an equality, $L \simeq R$, is defined if and only if the right-hand side is defined, and when they are defined, they are equal.

A *resource monoid* is a structure $\mathbf{R} = (\mathbf{R}, \circ, e, \sqsubseteq)$. We do not use a separate notation to distinguish the carrier set $\mathbf{R}$ from the structure. The structure has a preorder $\sqsubseteq$, a partial, binary operation $\circ$ and a distinguished element e. The operation $\circ$ satisfies monoid associativity and commutativity axioms up to Kleene equality. The unit of $\circ$ is e. Composition with this unit is always defined. Therefore, the structure satisfies the unit axiom for a commutative monoid up to actual equality. Resource monoids are further required to satisfy the *bifunctoriality condition*:

$$R \sqsubseteq R' \text{ and } S \sqsubseteq S' \text{ and } R' \circ S'\downarrow \quad \text{implies} \quad R \circ S\downarrow \text{ and } R \circ S \sqsubseteq R' \circ S' \tag{1}$$

for all R, R', S, S' in $\mathbf{R}$.

Some simple examples of resource monoids are:

1 The natural numbers with addition, zero and their usual order.
2 The real numbers with addition, zero and their usual order.
3 The set $\{0, 1\}$ with an operation $+$ such that $0 + 0 = 0$, $0 + 1 = 1 = 1 + 0$, $1 + 1\uparrow$ and the discrete order (equality).
4 A powerset $\mathscr{P}(L)$ of some set L. The composition is non-overlapping union: for any subsets X and Y of L, the composite $X \circ Y$ is defined just when $X \cap Y = \varnothing$, and, when defined, $X \circ Y = X \cup Y$. The unit is the empty set. The order is the discrete order.

The first example above is closely related to the kind of resources found in Demos2k; the third can be used as a kind of semaphore resource; and the fourth is what lies at the root of Separation Logic (Ishtiaq and O'Hearn 2001; Reynolds 2002).

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

Note that the order dual (obtained by reversing the order) of a resource monoid is not necessarily a resource monoid. Instead, it satisfies the property:

$$R \sqsubseteq R' \quad \text{and} \quad S \sqsubseteq S' \quad \text{and} \quad R \circ S \downarrow \quad \text{implies} \quad R' \circ S' \downarrow \quad \text{and} \quad R \circ S \sqsubseteq R' \circ S' \tag{2}$$

for all R, R', S, S' in $\mathbf{R}$. We define a resource monoid to be *special* when its dual is also a resource monoid, that is, when both (1) and (2) are satisfied. For the rest of this paper, the order $\sqsubseteq$ should be taken to be equality, except in Subsection 3.1 and Section 4.

A binary relation $\circledcirc$ between resources is important in the development of **SCRP**. Let R and S be resources. We say that S *piggybacks* on R, and write $S \circledcirc R$, if, for every resource T, if $R \circ T$ is defined, then $R \circ S \circ T$ is defined. Intuitively, $S \circledcirc R$ if whenever R is consistent with any T, then so is $R \circ S$. This predicate is used to ensure a well-behaved hiding operation. Note that if $S \circledcirc R$, then $R \circ S \downarrow$, and also that the relation $\circledcirc$ is total (that is, it holds for all pairs of resources) if and only if the composition operation is total.

We now set up a function describing how actions transform resources. A *modification* is a partial function $\mu : \mathsf{Act} \times \mathbf{R} \longrightarrow \mathbf{R}$ satisfying two *coherence* conditions:

1 $\mu(1, R) = R$ for all $R \in \mathbf{R}$.
2 If $\mu(a, R)$, $\mu(b, S)$ and $R \circ S$ are all defined, then $\mu(ab, R \circ S)$ and $\mu(a, R) \circ \mu(b, S)$ are both defined and $\mu(ab, R \circ S) = \mu(a, R) \circ \mu(b, S)$ holds.

Consider the resource monoid consisting of the natural numbers discussed above. Suppose that the action monoid is freely generated from a single action i, so every action can be represented in the form i^m for some unique integer $m \geqslant 0$. As a simple example of a modification function, consider

$$\mu(i^m, n) = m + n$$

for all natural numbers m and n. The action i is incrementation.

We assume a total operation called *hiding*, $\nu : \mathbf{R} \times \mathsf{Act} \longrightarrow \mathsf{Act}$, that takes any resource R and any action a and produces an action $\nu R.a$. The precise form of this operation is unimportant for most of the development that follows, and a number of possibilities exist. One such possibility was given in Pym and Tofts (2006; 2007) and Collinson *et al.* (2007) under the assumption that the action monoid is generated as a free monoid from a set of atomic actions. We reserve the letter α for atomic actions. Any action a may be written uniquely (up to re-ordering) as a product $a = \prod(\alpha_i \mid i \in I)$ for some family $(\alpha_i \mid i \in I)$ indexed by a finite set I. Then we may take

$$\nu S.a = \prod(\alpha_i \mid i \in I \ \&\ \mu(\alpha_i, S)\uparrow) \tag{3}$$

and recall that the product of an empty family of actions gives the identity action. The intuition behind this is that this resultant action $\nu S.a$ consists of precisely those atomic constituent actions α_i of a that play no role in the evolution of a process in the resource environment S, since $\mu(\alpha_i, S)$ is not defined, so the actions that fire when given S are hidden. The hiding processes introduced below only evolve along such actions $\nu S.a$, so any of their atoms that are enabled by S may not be externally observed. This is further clarified by the operational semantics of hiding processes described below.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

We assume a countable collection of *process variables*, for which the letter X is reserved. *Processes* are formed according to the grammar

$$E ::= 0 \mid X \mid a : E \mid \sum_{j \in J} E_j \mid E \times E \mid \nu R.E \mid fix_i \mathsf{X}.\mathsf{E},$$

where 0 is the *zero* process, X is a process variable, a is an action, J is an arbitrary index set, R is a resource, X is an n-tuple of process variables, E is an n-tuple of processes and $1 \leqslant i \leqslant n$. The letters E, F, G are reserved for processes, and the letters E, F, G for tuples of processes.

The *fix* operator binds occurrences of process variables within processes. It will occasionally be necessary to distinguish processes that contain no free variables (sometimes called *agents*) from the more general process expressions that exist in the language. We let Agents be the set of agents and Proc be the set of processes. Let X_i be the ith component of any tuple of process variables X, E_i be the ith component of any tuple of process expressions E of the same length. Then $F[\mathsf{E}/\mathsf{X}]$ is the process formed by the (capture-avoiding) substitution of each of the n components of E for the corresponding variable of X that is free in F. Similarly, there is substitution $\mathsf{F}[\mathsf{E}/\mathsf{X}]$ for the process variables in a tuple F. The expression $fix_i \mathsf{X}.\mathsf{E}$ means $(fix\, \mathsf{X}.\mathsf{E})_i$, the ith component of the tuple $fix\, \mathsf{X}.\mathsf{E}$. We use brackets, (), to disambiguate processes in the absence of their construction trees. The *unit* process 1 is defined to be $fix\, X.(1 : X)$. Given a sequence of the form $s = b_1/a_1, \ldots b_n/a_n$ with $a_1, \ldots, a_n$ distinct, the notation $E[s]$ stands for the process formed by the substitution of actions b_i for the actions a_i occurring in E.

With the exception of $\nu R.E$, these processes should appear familiar to those acquainted with process calculus. The calculus is intended to be a close relative of SCCS. Thus $a : E$ is a process with an action *prefix*, $\sum_{j \in J} E_j$ is a *sum*, $E \times F$ is a (*synchronous*) *product*, and $fix_i \mathsf{X}.\mathsf{E}$ is the ith component of the tuple of processes $fix\, \mathsf{X}.\mathsf{E}$ defined as a *fixed point*. The term $\nu R.E$ is a *hiding* process and is a resource-based form of restriction operation. We will often write binary sums using the infix notation $E + F$.

A *state* is a pair consisting of a resource and a process. Thus $\mathsf{States} = \mathbf{R} \times \mathsf{Proc}$ is the set of all states. We define the set $\mathsf{CStates}$ of *closed states* to consist of those states with an agent as the process component. If E is a process and R is any resource, we say that R, E is an *E-state*.

The operational behaviour of processes is defined by a labelled family of transition relations

$$\stackrel{a}{\rightarrow} \quad \subseteq \quad \mathsf{States} \times \mathsf{States}$$

indexed by $a \in \mathsf{Act}$. The family is defined recursively using the derivation rules of Figure 1. This describes how states evolve. Notice that the evolution of prefix processes with a given resource is completely determined by the modification μ. Product processes share out the globally available resources in such a way as to enable the components to evolve synchronously; the fact that the resulting composite $R' \circ S'$ appearing in the rule is well defined follows as an immediate consequence of the definition of modifications and Lemma 2 below. Essentially, a state $R, \nu S.E$ featuring a hiding process evolves along

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

Prefix $$\frac{}{R, a : E \xrightarrow{a} \mu(a, R), E} \qquad (\mu(a, R)\downarrow)$$

Sum $$\frac{R, E_j \xrightarrow{a} R', E'}{R, \sum_{j\in J} E_j \xrightarrow{a} R', E'} \qquad (j \in J)$$

Product $$\frac{R, E \xrightarrow{a} R', E' \qquad S, F \xrightarrow{b} S', F'}{R \circ S, E \times F \xrightarrow{ab} R' \circ S', E' \times F'} \qquad (R \circ S\downarrow)$$

Hide $$\frac{R \circ S, E \xrightarrow{a} R' \circ S', E'}{R, \nu S.E \xrightarrow{\nu S.a} R', \nu S'.E'} \qquad (\mu(\nu S.a, R) = R'\downarrow \ \& \ S \circledcirc R)$$

Fix $$\frac{R, E_i[fix\,\mathsf{X}.\mathsf{E}/\mathsf{X}] \xrightarrow{a} R', E'}{R, fix_i \mathsf{X}.\mathsf{E} \xrightarrow{a} R', E'}$$

Fig. 1. **SCRPr**-transitions

$\nu S.a$ when the underlying process E evolves along a given the resource formed $R \circ S$ by unpacking the hidden resource S.

The non-deterministic behaviour of processes is introduced into processes through the presence of sums. In most process calculi sums are the only source of non-determinism. In contrast, in **SCRP**-calculi non-determinism can also be introduced by instances of the product and hiding constructors. An arbitrary resource R can have many possible decompositions (R_1, R_2) such that $R = R_1 \circ R_2$. In such situations, a state of the form $R, E_1 \times E_2$ may make transitions induced by transitions of pairs of states $((R_1, E_1), (R_2, E_2))$ for each decomposition (R_1, R_2). Non-determinism is induced by hiding since, looking at the rule for hiding in Figure 1, there can be many possible resources S' such that the premise of the rule is true.

We define a (*state*) *derivative* of a state R, E to be a state R', E' that is reachable via a (possibly null) sequence of transitions. An *immediate* derivative is a state that can be reached using a single instance of a transition. A *proper derivative* is a derivative arising from a non-empty sequence of transitions. A *derivative* of a process E is any E' such that there are some R and R' such that R', E' is a derivative of R, E.

The system **SCRPr** is a restriction of the more general calculus **SCRP** originally suggested in Pym and Tofts (2006; 2007) and Collinson *et al.* (2007). The differences between the two systems are as follows:

1 The equality in the second clause in the definition of modification given above is replaced by a Kleene equality in **SCRP**.

2 The piggybacking condition does not appear in the side condition of the operational rule for hiding processes in **SCRP**.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

Clearly, **SCRP** applies to a wider range of situations than **SCRPr**. However, **SCRPr** has better operational behaviour and a closer correspondence with the logic **BI**.

2.2. *Structural properties*

The transition systems associated with **SCRPr** systems have a number of important properties. The following lemma is an immediate consequence of the operational semantics and is established by induction on derivations.

Lemma 1. If R, E is a state and E is an agent, then the process component of every derivative is an agent. In other words, the subspace CStates is closed under transitions.

The evolution of resources is entirely deterministic in the chosen action.

Lemma 2. If $R, E \xrightarrow{a} R', E'$, then $R' = \mu(a, R)$.

The proof of the lemma is an easy induction over derivations, and makes essential use of the coherence conditions on μ and the explicit and implicit side conditions on derivation rules.

The coherence properties for modifications lead immediately to a result for the extensibility of resources via composition.

Lemma 3. Let a be an action, and R and S be resources. If $\mu(a, R)$ and $R \circ S$ are defined, then $\mu(a, R \circ S) = \mu(a, R) \circ S$ is defined. We call this the *simple-extension* property for resources.

The existence of any transition from a state is closed under composition with further resources. That is, there is a simple-extension property for transitions as well as modifications.

Proposition 4. Let E be a process, a be an action, and R and S be resources. If $R, E \xrightarrow{a} \mu(a, R), E'$ and $R \circ S$ is defined, then $R \circ S, E \xrightarrow{a} \mu(a, R) \circ S, E'$.

The proof of the above proposition is an easy induction over derivations of transitions. Lemma 3 establishes the base case (Prefix) and the side condition on piggybacking ensures that the induction passes across the Hide case.

By an analogy with situations that arise in Proof Theory, this can be seen as establishing an *admissible rule*:

$$\frac{R, E \xrightarrow{a} \mu(a, R), E'}{R \circ S, E \xrightarrow{a} \mu(a, R) \circ S, E'} \qquad (R \circ S \downarrow)$$

for all suitable R, S, E, E', a. This is rather like a weakening rule for the resource component of a state. Many other structural rules can, of course, be considered, and their admissibility is linked to the structure of the underlying resource monoid. When such rules are not admissible (for example, if we forget about piggybacking when hiding), one may choose to include them explicitly in the calculus as the algebraic and logical properties of these kinds of calculi sometimes rely critically upon their presence.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

2.3. *Bisimulation*

It is usual to have a notion of equality for process terms that treats processes with the same behaviour as equal. The standard notion is that of an equivalence relation called *bisimulation*. For calculi in the **SCRP** family the situation is a little delicate. First, there is a question about where the equivalence should live. On the one hand, simulation is usually defined via transition structures, see, for example, Milner (1983) and Popkorn (1994). This suggests an equivalence between states, that is, between systems or models. On the other hand, an equivalence of processes is probably more useful than an equivalence of states, as this is the part of a system in which it is most natural to exercise control. Furthermore, the compositional nature of the systems we build resides primarily in the process part, and we frequently want to know that two processes behave in the same way in any given resource context. We explore these issues carefully for the calculus **SCRPr**, and with an eye on logical equivalence of processes, as well as behavioural equivalence of processes and states.

We define the *local equivalence* relation $\approx$ to be the largest binary relation on closed states such that the following condition holds. Let R and S be resources and E and F be processes. If $R, E \approx S, F$, then:

1 If there is a transition $R, E \xrightarrow{a} \mu(a, R), E'$ for any E', then there is transition $R, F \xrightarrow{a} \mu(a, R), F'$ with $\mu(a, R), E' \approx \mu(a, R), F'$ for some F'.

2 If there is a transition $R, F \xrightarrow{a} \mu(a, R), F'$ for any F', then there is a transition $R, E \xrightarrow{a} \mu(a, R), E'$ with $\mu(a, R), E' \approx \mu(a, R), F'$ for some E'.

3 $R = S$.

The relation $\approx$ is extended to all states by substitution: for any states R, E and S, F we define $R, E \approx S, F$ if and only if $R, E[\mathsf{G}/\mathsf{X}] \approx S, F[\mathsf{G}/\mathsf{X}]$ for all m-tuples of agents G, where X is an m-tuple representing the set of free variables of E and F.

This relation $\approx$ is almost the same as that considered in Pym and Tofts (2006; 2007) and Collinson *et al.* (2007). Note, however, that we have defined the relation initially for agents rather than for arbitrary process expressions, and that this gives a slightly smaller relation.

Fundamentally, this relation starts from the view that agents should be considered equivalent whenever they have the same behaviour given the same resources. Pym and Tofts (2007) showed that this relation is intimately connected to a denotational semantics of **SCRP** that uses synchronisation trees. Indeed, the relation on closed states looks very much like the standard notion of bisimulation for transition structures, see Popkorn (1994), for example. In view of Lemma 2, the main difference is the insistence that the resource components of the states under comparison are identical. Clearly, local equivalence on closed states is contained in the standard kind of bisimulation for transition systems on those states. Consequently, a modal logic of system properties may be expected. However, the local equivalence relation fails to be a congruence as it is not respected by the product constructor for processes – the references Pym and Tofts (2006; 2007) contain an error on this point.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

Example 5. Consider the resource monoid $(\mathbb{N}, +, 0)$ consisting of the natural numbers with addition. Let Act be the monoid of actions freely generated from a single action d. Every element of Act has the form d^i for some unique $i \in \mathbb{N}$. There is a modification defined by

$$\mu(d^i, n) = \begin{cases} n - i & \text{if } i \leqslant n \\ \uparrow & \text{otherwise} \end{cases}$$

for all $i, n \in \mathbb{N}$. Let E be the process $d : \mathsf{0}$, let F be $\mathsf{0}$ and let G be $1 : \mathsf{0}$.

Then $0, E \approx 0, F$ holds since neither state makes any transitions. However, the relation $0 + 1, E \times G \approx 0 + 1, F \times G$ does not hold, since $1, E \times G$ has a transition but $1, F \times G$ does not.

We write $E \approx F$ whenever $R, E \approx R, F$ for all resources R. This relation is an equivalence, but not a congruence.

Example 6. Let L be a set of locations. Let a *heap* be a partial function from L to the set $\mathbb{N}$ of integers. We define the composite of a pair of heaps by taking the non-overlapping union of their graphs. Let $dom(h) = \{x \in L \mid h(x)\downarrow\}$ for any heap h. Then, for any heaps h and h', the composite $h \circ h'$ is defined if and only if $dom(h) \cap dom(h') = \varnothing$. Furthermore, $(h \circ h')(x) = h(x)$ if $x \in dom(h)$, and $(h \circ h')(x) = h'(x)$ if $x \in dom(h')$. The unit heap is the empty partial function. In this way, the set of heaps forms a resource monoid.

Let $x_1, \ldots, x_n$ be distinct locations and $z_1, \ldots, z_n$ be integers. For any heap h, we define a heap $h' = h[x_1 := z_1, \ldots, x_n := z_n]$ as follows:

$$h'(x) = \begin{cases} \uparrow & \text{if } h(x) \uparrow \\ z_i & \text{if } h(x) \downarrow \text{ and } x = x_i \text{ for some } 1 \leqslant i \leqslant n \\ h(x) & \text{otherwise.} \end{cases}$$

Let the action monoid Act be freely generated from the actions $a_{x,z}$ and $b_{x,z}$ for all $x \in L$ and $z \in \mathbb{N}$. Let 1 be the unit action.

Let c be any action. This may be written uniquely (up to re-ordering) in the canonical form

$$a_{x_1,z_1}^{m_1} \cdots a_{x_n,z_n}^{m_n} b_{x_{n+1},z_{n+1}}^{m_{n+1}} \cdots b_{x_{n+p},z_{n+p}}^{m_{n+p}}$$

for some $n, p \geqslant 0$, where each $m_i > 0$, and each pair x_i, z_i appears at most once as the subscript of an a-atom, and at most once as the subscript of a b-atom.

We take $\mu(c, h)$ to be defined if and only if, in the canonical form above, $x_i \neq x_j$ for all x_i, x_j that appear, $m_i = 1$ for all m_i that appear, and $h(x_i)\downarrow$ for all x_i that appear. If $\mu(c, h)$ is defined, then

$$\mu(c, h) = h[x_1 := z_1, \ldots, x_n := z_n].$$

Note that $\mu(a_{x,z}, h)$ is defined if $h(x)$ is defined, and then $\mu(a_{x,z}, h) = h[x := z]$, so $a_{x,z}$ is the action $x := z$ that updates the heap with the value z at location x. Similarly, $\mu(b_{x,z}, h)$ is defined if $h(x) = z$ is defined, and then $\mu(b_{x,z}, h) = h$, so $b_{x,z}$ is the guard $x = z$. The modification at the action c above is undefined whenever two atoms in c use the same location.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

Consider the processes

$$E = b_{x,0} : 1 : (1 : 0 + b_{x,1} : 0) \qquad F = b_{x,0} : 1 : 1 : 0$$

for some fixed location x. These two processes satisfy

$$E \approx F$$

because if the first guard $x = 0$ in E is true at any h, then the second guard $x = 1$ must be false, so the two processes generate the same transition structures.

Let

$$G = 1 : a_{x,1} : 1 : 0$$

and let h_0 be the heap defined only at location x, and such that $h_0(x) = 0$. Then we do not have $h_0, E \times G \approx h_0, F \times G$, since $h_0, E \times G$ may eventually perform the $b_{x,1}$ action, but $h_0, F \times G$ cannot. Hence

$$E \times G \not\approx F \times G$$

holds. Therefore, the relation $\approx$ on processes is not a congruence for the product constructor.

The relation $\approx$ on processes also fails to be closed under transitions in the sense that we can have $E \approx F$ and $R, E \xrightarrow{a} \mu(a, R), E'$ for some E' and R, but no corresponding F' with $R, F \xrightarrow{a} \mu(a, R), F'$ and $E' \approx F'$. This means that the relation $\approx$ does not interact well with the modal logic we introduce below (the more natural relation for which seems to be $\approx$ on states). We believe it would be worth exploring a version of $\approx$ on states in which the resource components need not be identical. This topic, which we suspect may be quite difficult, is suggested on the one hand by a desire to compare *systems*, and on the other by the general notion of bisimulation in modal logic (Popkorn 1994).

There is a natural alternative relation, which is a congruence but is defined initially on agents rather than states. We define the *global equivalence* relation $\sim$ to be the largest relation binary on agents such that, whenever $E \sim F$ holds:

1 If $R, E \xrightarrow{a} \mu(a, R), E'$ for any R, E', then there is some F' with $R, F \xrightarrow{a} \mu(a, R), F'$ and $E' \sim F'$.
2 If $R, F \xrightarrow{a} \mu(a, R), F'$ for any R, F', then there is some E' with $R, E \xrightarrow{a} \mu(a, R), E'$ and $E' \sim F'$.

The relation $\sim$ is then extended to all tuples of processes by substitution: for any n-tuples of processes E and F, we define $\mathsf{E} \sim \mathsf{F}$ if and only if $E_i[\mathsf{G}/\mathsf{X}] \sim F_i[\mathsf{G}/\mathsf{X}]$ for all $1 \leqslant i \leqslant n$ and all m-tuples of agents G, where X is any m-tuple containing the free variables of E and F with each listed exactly once. The global equivalence is lifted to states by taking $R, E \sim R, F$ to hold just when $E \sim F$ for all E, F and R.

The global equivalence is intimately related to the logical language **MBIc** based on resource semantics that we develop in Section 3. Notice that for a local equivalence $E \approx F$, it is enough to compare derivatives of states R, E and R, F for all initial resources R. In contrast, for a global equivalence, one must also compare states of the form S, E' and S, F' that are resource perturbations of derivatives of the form R', E' and R', F' of R, E and R, F for any R. That is to say, for global equivalence we cannot just compare derivatives,

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

we must also compare states that arise by perturbing the resource component of such derivatives.

Proposition 7. The relation $\sim$ on processes is a congruence. That is, it is an equivalence relation that is respected by the process constructors. In particular, if $E \sim F$ between processes and $\mathsf{E} \sim \mathsf{F}$ between n-tuples of processes, then for any action a, process G, resource S, n-tuple X and index i:

$$a : E \sim a : F$$

$$E + G \sim F + G \qquad E \times G \sim F \times G$$

$$\nu S.E \sim \nu S.F \qquad fix_i \mathsf{X}.\mathsf{E} \sim fix_i \mathsf{X}.\mathsf{F}.$$

Proof. The reflexivity, symmetry and transitivity of the relation are all straightforward.

The proofs of the equalities stated above are also quite standard. For example, consider the set of pairs of agents $A = \{(E \times G, F \times G) \mid E \sim F\}$. Consider some pair $(E \times G, F \times G) \in A$. Consider any R and suppose that there is a transition $R, E \times G \xrightarrow{a} \mu(a, R), E_1$ for some E'. Then E_1 must be of the form $E' \times G'$, and there must be some actions b, c with $a = bc$ and some resources S, T with $R = S \circ T$ such that $S, E \xrightarrow{b} \mu(b, S), E'$ and $T, G \xrightarrow{c} \mu(c, T), G'$. Since $E \sim F$, there must be a transition $S, F \xrightarrow{b} \mu(b, S), F'$ for some F' with $E' \sim F'$. Hence, there is a transition $R, F \times G \xrightarrow{a} \mu(a, R), F' \times G'$ and $(E' \times G', F' \times G') \in A$. The symmetry of the components of the elements of set A then shows that $E \times G \sim F \times G$. The result then immediately lifts to processes.

Just as in Milner (1983, Proposition 4.6), the congruence property for the fixed point relies on the way that the relation has been lifted from agents to processes and uses the preceding equalities. □

We omit the proofs of the following two lemmas since they are routine verifications – the first is established by showing that $\sim$ on closed states is closed under the conditions for a local equivalence.

Lemma 8. The global equivalence relation $\sim$ on closed states is contained in the local equivalence relation $\approx$ on such states.

We shall see that this is important for the modal logic **MBIc**. The relation $\approx$ on states is not a congruence and so cannot be contained in the relation $\sim$ on states.

We use the notations $\lesssim$ and $\lessapprox$ in the standard way for the asymmetric variants of $\sim$ and $\approx$. Thus, for example, $R, E \lessapprox R, F$ just if whenever the agent R, E makes some transition into some R', E', then the agent R, F makes a transition along the same action and into a state R', F' with $R', E' \lessapprox R', F'$. We now return to the question of algebraic identities.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

Lemma 9. The following simple equalities and inequalities hold for the relation $\sim$ on processes:

$$E \times F \sim F \times E \qquad E \times (F \times G) \sim (E \times F) \times G$$

$$E + F \sim F + E \qquad E + (F + G) \sim (E + F) + G$$

$$E \times 0 \sim 0 \qquad E \times 1 \sim E$$

$$E + 0 \sim E \qquad E + E \sim E$$

$$E \times (F + G) \sim (E \times F) + (E \times G) \qquad \nu S.(E + F) \sim (\nu S.E) + (\nu S.F)$$

$$(a : E) + (a : F) \lesssim a : (E + F) \qquad (a : E) \times (b : F) \lesssim (ab) : (E \times F)$$

for all processes E, F and G.

Proof. Again, it suffices to show the result on agents. The rest is straightforward verification using the fact that $\sim$ on closed states is defined to be the largest relation closed under the given conditions. It is important to note that the property $E \times 1 \sim E$ needs the simple-extension property for transitions (Proposition 4). □

All of the simple algebraic identities from Lemma 9 hold with $\sim$ replaced by $\approx$ throughout: this follows immediately from the fact that $\sim$ is contained in $\approx$.

Further inequalities may well hold for specific choices of resource monoid, modification, hiding and action set. For example, well-behaved hiding on actions leads to better-behaved hiding processes.

Lemma 10. If $\nu(S \circ T).a = \nu S.\nu T.a$ for all actions a and any resources S and T, then the relation $\nu S.\nu T.E \lesssim \nu(S \circ T).E$ holds for any process E.

However, the following two properties *do not* hold in general:

1 $R, a : (E + F) \lessapprox R, a : E + a : F$.
2 $R, (ab) : (E \times F) \lessapprox R, (a : E) \times (b : F)$.

Simple counterexamples exist for each. Of course, if $R, F \lessapprox R, E$, then $R, F \lesssim R, E$ for any R, E, F. To see that the first point does not hold, consider any pair of states $R, a : E + a : F$ and $R, a : (E + F)$ with $a = 1$, $E = 1 : 0$ and $F = 0$. For the second, consider the trivial resource monoid $\mathbb{N}$ with addition, action monoid generated from the set $\{a, b\}$ and modification satisfying $\mu(a^m b^n, p) = p + n - m$ if $m \leqslant p + n$ and that is undefined otherwise. Then $\mu(ab, 0)$ is defined but $\mu(a, 0)$ is undefined, so there is an ab-transition of the prefix process $ab : (0 \times 0)$ but no transition of the product $(a : 0) \times (b : 0)$.

The following lemma gives an important representation of any state.

Lemma 11. Let E be any process. For any resource R, we may write,

$$R, E \approx R, \sum \{a : E' \mid R, E \xrightarrow{a} \mu(a, R), E'\}$$

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

and, furthermore,

$$\sum\{a : E' \mid \forall R.\ R, E \xrightarrow{a} \mu(a, R), E'\} \lesssim E \lesssim \sum\{a : E' \mid \exists R.\ R, E \xrightarrow{a} \mu(a, R), E'\}$$

holds.

Proof. For the first part, the transitions and immediate derivatives on the left are precisely the same as those on the right. □

This result specialises in the case of a product of processes.

Lemma 12.

$$R, E_1 \times \ldots \times E_n \approx R, \sum\{(a_1 \cdots a_n).(E_1' \times \ldots \times E_n') \mid \exists R_1, \ldots, R_n.\ R = R_1 \circ \ldots \circ R_n \ \&\ \forall 1 \leqslant i \leqslant n.\ R_i, E_i \xrightarrow{a_i} \mu(a_i, R_i), E_i'\ \}.$$

Proof. The coherence conditions on modifications guarantee that a transition on the left is a transition on the right into the same derivative. The indexing set on the right guarantees that there are no more transitions on the right. □

We may expand out hiding processes in a similar way.

Lemma 13.

$$R, \nu S.E \approx R, \sum\{(\nu S.a) : (\nu S'.E') \mid R \circ S, E \xrightarrow{a} R' \circ S', E' \ \&\ \mu(\nu S.a, R) = R' \ \&\ S \Subset R\ \}.$$

In the special case of a prefix,

$$R, \nu S.(a : E) \approx R, \sum\{(\nu S.a) : (\nu S'.E') \mid \mu(a, R \circ S) = \mu(\nu S.a, R) \circ S' \ \&\ S \Subset R\ \}.$$

Proof. For any given resource, the derivatives of the left-hand side coincide exactly with the derivatives of the right-hand side. □

The preceding results can be combined to give the *local expansion theorem* for states in the synchronous calculus.

Theorem 14.

$$R, \nu S.(E_1 \times \ldots \times E_n) \approx R, \sum\{\nu S.(a_1 \ldots a_n).\nu S'.(E_1' \times \ldots \times E_n') \mid S \Subset R\ \&\ \exists R_1, \ldots, R_n.\ R \circ S = R_1 \circ \ldots \circ R_n\ \&\ \mu(a_1 \ldots a_n, R \circ S) = \mu(\nu S.(a_1 \ldots a_n), R) \circ S'\ \&\ \forall 1 \leqslant i \leqslant n.\ R_i, E_i \xrightarrow{a_i} \mu(a_i, R_i), E_i'\}.$$

Proof. Notice that if $S \Subset R$ does not hold, then the sum on the right is empty and this gives the process $\mathsf{0}$. Once again, a transition to a derivative on the left exists if and only if it exists on the right. The result generalises easily to a form with multiple hidings (rather than just one) outermost in the process term. □

It is rather unsatisfactory to have these results stated only for $\approx$, given that it fails to be a congruence. One would like to have an expansion theorem for processes, and preferably using $\sim$. However, this does not seem to be possible in the general case, even using $\approx$. The expansion relies critically on the resource at which the expansion is performed. In

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

particular, the second part of Lemma 11 cannot be tightened to make the second of the inequalities an equality, because there can exist processes E and E', and resources R and S, with $R, E \xrightarrow{a} \mu(a, R), E'$ and $\mu(a, S)$ defined, but such that there is no transition $S, E \xrightarrow{a} \mu(a, S), E'$.

2.4. *Specifying modifications*

General methods are needed for specifying modifications. It is not always feasible to specify the modification function individually at all actions and all resources. Furthermore, when such a specification is made, the function defined must be explicitly checked to satisfy the coherence conditions.

One method that can often be employed is to specify the modification on atomic actions. Under suitable conditions this gives rise to a unique coherent modification. The conditions we use involve the preorder that arises from the composition. For the purposes of this section, we assume that we are working with an action monoid that is freely generated from some set of atomic actions.

We will often suppose that we are working with a resource monoid $\mathbf{R}$ with *cancellation*, that is, the partial function $S \circ (-) : \mathbf{R} \longrightarrow \mathbf{R}$ is injective for every S. In other words, for any R and S, if whenever $R = S \circ T$ for some T, that T is unique. We usually write T as $R - S$. We define a resource monoid to be *good* when it has cancellation and composition is total. We define the preorder $\sqsubseteq$ by

$$S \sqsubseteq R \qquad \Longleftrightarrow \qquad \exists T. \quad S \circ T = R$$

for all resources R and S.

We define a partial function $f : \mathbf{R} \longrightarrow \mathbf{R}$ to be *rooted* if:

1 There is a unique resource R_0, called the *root*, such that for all R, $f(R)$ is defined if and only if $R_0 \sqsubseteq R$.
2 For all R and S, if $f(R)$ and $R \circ S$ are defined, then $f(R \circ S) = f(R) \circ S$ is defined.

The following lemma is then immediate. Indeed, it characterises rooted functions on good monoids.

Lemma 15. For any rooted function f on a good resource monoid,

$$f(R) \simeq f(R_0) \circ (R - R_0)$$

for all resources R, where R_0 is the root of f.

We define an Act-indexed family of resources $(R_a \mid a \in \mathsf{Act})$ to be *consistent* if for any two actions a and b,

$$R_{ab} = R_a \circ R_b$$

holds.

Lemma 16. Every consistent family of resources on a good resource monoid satisfies

$$(R \circ S) - R_{ab} = (R - R_a) \circ (S - R_b)$$

for all a, b, R, S such that the right-hand side is defined.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

Proof. Consider the calculation

$$\begin{aligned}((R - R_a) \circ (S - R_b)) \circ R_{ab} &= (R - R_a) \circ (S - R_b) \circ R_a \circ R_b \\ &= R \circ S\end{aligned}$$

for any given R, R, a, b. The uniqueness of $(R \circ S) - R_{ab}$ then gives the result. □

Suppose that we have a family of resources R_α indexed by atomic actions, with each member drawn from the same good resource monoid. We extend the family to a family indexed by all actions by taking

$$R_a = \bigcirc_{1 \leqslant i \leqslant n} R_{\alpha_i}$$

for all $a = \alpha_1 \ldots \alpha_n$, where $n = 0$ is the special case for the unit action, and $\bigcirc_{i \in I}$ is I-indexed resource composition for any finite set I. Note that $R_1 = e$. The proof of the following lemma is then a routine verification.

Lemma 17. The Act-indexed family of resources generated (as above) from the family of resources indexed by atomic actions is consistent.

We now return to the issue of functions specified at actions.

Proposition 18. Suppose we have a good resource monoid and a family of rooted, partial functions $\mu_\alpha : \mathbf{R} \longrightarrow \mathbf{R}$ indexed by atomic actions α, and that the root of each μ_α is R_α. Then there is a unique modification $\mu : \mathsf{Act} \times \mathbf{R} \longrightarrow \mathbf{R}$ such that

$$\mu(\alpha, R) \simeq \mu_\alpha(R) \tag{4}$$

for all atomic actions α and all resources R. Note that the equality here is a Kleene equality. Moreover, this satisfies

$$\mu(a, R) = \begin{cases} \mu(a, R_a) \circ (R - R_a) & \text{if } R_a \sqsubseteq R \\ \uparrow & \text{otherwise} \end{cases} \tag{5}$$

for all actions a and resources R, where the consistent family $(R_a \mid a \in \mathsf{Act})$ is generated from the family of roots R_α indexed by atomic actions.

Proof. For any atomic action α and resource R,

$$\mu_\alpha(R) = \begin{cases} \mu_\alpha(R_\alpha) \circ (R - R_\alpha) & \text{if } R_\alpha \sqsubseteq R \\ \uparrow & \text{otherwise} \end{cases}$$

since μ_α is rooted. For every $n \geqslant 1$, take

$$\mu(\alpha_1 \ldots \alpha_n, R) = \begin{cases} \mu(\alpha_1, R_{\alpha_1}) \circ \ldots \circ \mu(\alpha_n, R_{\alpha_n}) \circ (R - R_{\alpha_1 \ldots \alpha_n}) & \text{if } R_{\alpha_1 \ldots \alpha_n} \sqsubseteq R \\ \uparrow & \text{otherwise} \end{cases} \tag{6}$$

for every sequence of atoms $\alpha_1, \ldots, \alpha_n$ and resource R. It is straightforward, using Lemmas 16 and 17, to verify that this is coherent and satisfies equations (4) and (5). For uniqueness, observe that the coherence property requires equation (6). □

The proposition tells us how to construct a modification from a specification on atoms. In practical modelling, many resource monoids are indeed good and modifications are (implicitly) specified through a small family of rooted functions. This is also connected

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

to the enabling functions discussed in Pym and Tofts (2006), which we shall return to in Section 4.

We sometimes need to define a modification by specifying it on atomic actions as above, but where each atom does not have a unique root, and when resource composition is not required to be total. We now show how to get a **SCRP**-modification in such a situation. This may not always be a **SCRPr**-modification, and we only show that it satisfies the Kleene-equality version of the second coherence condition.

For the remainder of this section, we assume that **R** is a resource monoid with cancellation, but for which composition is not necessarily total.

Lemma 19.

$$R - (S \circ T) \simeq (R - S) - T \simeq (R - T) - S$$

for all resources R, S, T.

Proof. Suppose $(R-(S\circ T))$ is defined. Then $(R-(S\circ T))\circ S\circ T = R$, so $(R-(S\circ T))\circ S = R - T$, and then $(R - (S \circ T)) = (R - T) - S$.

Suppose $(R - T) - S$ is defined. Then $((R - T) - S) \circ S = R - T$ is defined, so $((R - T) - S) \circ S \circ T = R$. Then, by definition, $((R - T) - S) = R - (S \circ T)$. □

Lemma 20. If $R \circ S$ and $R - T$ are defined, then $(R \circ S) - T = (R - T) \circ S$ is defined.

Proof. The calculation

$$((R - T) \circ S) \circ T = ((R - T) \circ T) \circ S = R \circ S$$

gives the result. □

Lemma 21. If $(R - R_1)$, $(S - S_1)$ and $R \circ S$ are defined,

$$(R - R_1) \circ (S - S_1) \simeq (R \circ S) - (R_1 \circ S_1).$$

Proof. Suppose $(R - R_1) \circ (S - S_1)$ is defined. Then

$$(R - R_1) \circ (S - S_1) \circ R_1 \circ S_1 = R \circ S$$

is defined. So

$$(R - R_1) \circ (S - S_1) = (R \circ S) - (R_1 \circ S_1).$$

Now suppose $(R \circ S) - (R_1 \circ S_1)$ is defined. Then

$$((R \circ S) - (R_1 \circ S_1)) \circ (R_1 \circ S_1) = R \circ S$$

is defined, and thus

$$((R \circ S) - (R_1 \circ S_1)) \circ S_1 = (R \circ S) - R_1$$

is defined. By Lemma 20,

$$((R \circ S) - (R_1 \circ S_1)) \circ S_1 = (R - R_1) \circ S,$$

so

$$(R \circ S) - (R_1 \circ S_1) = ((R - R_1) \circ S) - S_1$$

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

is defined. Hence

$$(R \circ S) - (R_1 \circ S_1) = (R - R_1) \circ (S - S_1)$$

by Lemma 20. □

A partial function $f : \mathbf{R} \longrightarrow \mathbf{R}$ is said to be *multi-rooted* if there is a set A, called the *set of roots* of f, such that:

1 $f(R_0)$ is defined, for all $R_0 \in A$.
2 For all R, $f(R)$ is defined if and only if there is some $R_0 \in A$ such that $f(R_0) \circ (R - R_0)$ is defined and $f(R) = f(R_0) \circ (R - R_0)$.
3 The set of roots is coherent:

$$f(R_1) \circ (R - R_1) = f(R_2) \circ (R - R_2)$$

for all roots $R_1, R_2 \in A$ and all R such that $f(R_1) \circ (R - R_1)$ and $f(R_2) \circ (R - R_2)$ are defined.

Proposition 22. Let **R** be a resource monoid with cancellation. Suppose there is a family of multi-rooted partial functions μ_α indexed by atomic actions α. For each atomic α, let $\mathsf{Roots}(\alpha)$ be the set of roots of μ_α. Then there is a **SCRP**-modification on **R** defined as follows. At any resource R and action $a = \alpha_1 \cdots \alpha_n \neq 1$,

$$\mu(\alpha_1 \cdots \alpha_n, R) = \mu_{\alpha_1}(R_1) \circ \ldots \circ \mu_{\alpha_n}(R_n) \circ (R - (R_1 \circ \ldots \circ R_n))$$

if there are $R_i \in \mathsf{Roots}(\alpha_i)$ for $1 \leqslant i \leqslant n$ such that the right-hand side is defined, otherwise we take $\mu(\alpha_1 \cdots \alpha_n, R)$ to be undefined. If $a = 1$, then $n = 0$, and we take $\mu(1, R) = R$.

Proof. We first show that $\mu(a, -)$ is well defined as a partial function by induction on the number n of actions in $a = \alpha_1 \cdots \alpha_n$.

Suppose $n = 1$ and R_1 and S_1 are both roots of μ_{α_1} such that $\mu_{\alpha_1}(R) \circ (R - R_1)$ and $\mu_{\alpha_1}(S_1) \circ (R - S_1)$ are both defined for some R. Then, by the coherence of the roots of μ_{α_1}, we have $\mu_{\alpha_1}(R) \circ (R - R_1) = \mu_{\alpha_1}(S_1) \circ (R - S_1)$, so $\mu(\alpha_1, R)$ is unambiguous.

Suppose the result holds for $\alpha_1 \cdots \alpha_n$ and consider $a = \alpha_1 \cdots \alpha_{n+1}$. Suppose there is a resource R and roots $R_i, S_i \in \mathsf{Roots}(\alpha_i)$ for $1 \leqslant i \leqslant n$ with

$$\mu_{\alpha_1}(R_1) \circ \ldots \circ \mu_{\alpha_n}(R_n) \circ \mu_{\alpha_{n+1}}(R_{n+1}) \circ (R - (R_1 \circ \ldots \circ R_n \circ R_{n+1}))$$

and

$$\mu_{\alpha_1}(S_1) \circ \ldots \circ \mu_{\alpha_n}(S_n) \circ \mu_{\alpha_{n+1}}(S_{n+1}) \circ (R - (S_1 \circ \ldots \circ S_n \circ S_{n+1}))$$

both defined. Then

$$\begin{aligned}
&\mu_{\alpha_1}(R_1) \circ \ldots \circ \mu_{\alpha_n}(R_n) \circ \mu_{\alpha_{n+1}}(R_{n+1}) \circ (R - (R_1 \circ \ldots \circ R_n \circ R_{n+1})) \\
&\quad = \mu_{\alpha_1}(R_1) \circ \ldots \circ \mu_{\alpha_n}(R_n) \circ \mu_{\alpha_{n+1}}(R_{n+1}) \circ ((R - (R_1 \circ \ldots \circ R_n)) - R_{n+1}) \\
&\quad = \mu_{\alpha_1}(R_1) \circ \ldots \circ \mu_{\alpha_n}(R_n) \circ \mu_{\alpha_{n+1}}(S_{n+1}) \circ ((R - (R_1 \circ \ldots \circ R_n)) - S_{n+1}) \\
&\quad = \mu_{\alpha_1}(R_1) \circ \ldots \circ \mu_{\alpha_n}(R_n) \circ ((R - S_{n+1}) - (R_1 \circ \ldots \circ R_n)) \circ \mu_{\alpha_{n+1}}(S_{n+1}) \\
&\quad = \mu_{\alpha_1}(S_1) \circ \ldots \circ \mu_{\alpha_n}(S_n) \circ ((R - S_{n+1}) - (S_1 \circ \ldots \circ S_n)) \circ \mu_{\alpha_{n+1}}(S_{n+1}) \\
&\quad = \mu_{\alpha_1}(S_1) \circ \ldots \circ \mu_{\alpha_n}(S_n) \circ \mu_{\alpha_{n+1}}(S_{n+1}) \circ (R - (S_1 \circ \ldots \circ S_n \circ S_{n+1})),
\end{aligned}$$

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

where we have used Lemma 19 three times, the induction hypothesis and the fact that $\mu_{\alpha_{n+1}}$ is rooted and

$$\mu_{\alpha_{n+1}}(R_{n+1}) \circ ((R - (S_1 \circ \ldots \circ S_n)) - R_{n+1}))$$

and

$$\mu_{\alpha_{n+1}}(S_{n+1}) \circ ((R - (S_1 \circ \ldots \circ S_n)) - S_{n+1}))$$

are both defined.

Suppose $\mu(a, R)$, $\mu(b, S)$ and $R \circ S$ are all defined. If both of the actions are the unit, then $\mu(ab, R \circ S) = \mu(1, R \circ S) = R \circ S = \mu(a, R) \circ \mu(b, S)$ are all defined. Consider the case where just one of the actions is the unit – without loss of generality, we can suppose that it is b. Then, for some atoms $\alpha_1, \ldots, \alpha_n$ and resources $R_1, \ldots, R_n$,

$$\begin{aligned}
\mu(a, R) \circ \mu(b, S) &\simeq \mu(a, R) \circ S \\
&\simeq \mu_{\alpha_1}(R_1) \circ \ldots \circ \mu_{\alpha_m}(R_m) \circ (R - (R_1 \circ \ldots \circ R_m)) \circ S \\
&\simeq \mu_{\alpha_1}(R_1) \circ \ldots \circ \mu_{\alpha_m}(R_m) \circ ((R \circ S) - (R_1 \circ \ldots \circ R_m)) \\
&\simeq \mu(ab, R \circ S)
\end{aligned}$$

using Lemma 20. Now suppose $a = \alpha_1 \cdots \alpha_m$ and $b = \beta_1 \cdots \beta_n$. Then

$$\begin{aligned}
\mu(a, R) \circ \mu(b, S) &\simeq \mu_{\alpha_1}(R_1) \circ \ldots \circ \mu_{\alpha_m}(R_m) \circ (R - (R_1 \circ \ldots \circ R_m)) \circ \\
&\quad \mu_{\beta_1}(S_1) \circ \ldots \circ \mu_{\beta_n}(S_n) \circ (S - (S_1 \circ \ldots \circ S_n)) \\
&\simeq \mu_{\alpha_1}(R_1) \circ \ldots \circ \mu_{\alpha_m}(R_m) \circ \mu_{\beta_1}(S_1) \circ \ldots \circ \mu_{\beta_n}(S_n) \circ \\
&\quad ((R \circ S) - ((R_1 \circ \ldots \circ R_m) \circ (S_1 \circ \ldots \circ S_n))) \\
&\simeq \mu(ab, R \circ S)
\end{aligned}$$

using Lemma 21, and roots $R_i \in \mathsf{Roots}(\alpha_i)$, $S_j \in \mathsf{Roots}(\beta_j)$ for all $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$. Thus μ satisfies the conditions for a modification of **SCRP**. □

3. Bunched modal logic

The logic **MBI** was sketched, with some basic properties, in Pym and Tofts (2006; 2007) and Collinson *et al.* (2007). **MBI** is a modal logic resembling Hennessy–Milner logic (Hennessy and Milner 1985) and based on bunched logic (O'Hearn and Pym 1999; Pym 1999; Pym *et al.* 2004; Pym 2002). As such, it serves as a specification language for the process algebra **SCRP**.

The logic **MBI** has been shown to give a logical account of process constructs: in particular, synchronous product and hiding. It has also been shown through a number of key examples to give a useful account of resource use by concurrent processes. In this section we present a more developed account.

The logic as presented in Pym and Tofts (2006; 2007) and Collinson *et al.* (2007) is not equipped with a (proof-theoretic) deductive system. Here we give a proof system for (propositional) **MBI** that adds modal axioms to (propositional) **BI**'s natural deduction system (O'Hearn and Pym 1999; Pym 1999; 2002). The logical calculus has a number of important properties that follow from the properties of the **SCRPr** calculus – these properties were not all present in the previous accounts.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

3.1. *Bunched implications*

The logical system we wish to consider is based on propositional **BI**, the logic of bunched implications. Here we present a brief review – more detailed accounts may be found in O'Hearn and Pym (1999), Pym (1999), Pym *et al.* (2004) and Pym (2002).

The logic **BI** combines a logic with structural rules of contraction and weakening (intuitionistic logic) with a substructural logic that lacks these rules (multiplicative linear logic). Furthermore, it does this in such a way that the two embedded logics have the same status (neither is definable from the other) and so that certain properties of those logics are retained. The composite logic provides two variants, additive and multiplicative, of several of the basic logical connectives. These have clear and distinct interpretations on resource monoids, which gives rise to many applications. An example of this is Separation Logic (Ishtiaq and O'Hearn 2001; Reynolds 2002), which is a Floyd–Hoare-style program logic with local reasoning regarding state.

We assume a set Prop_0 of basic propositions φ. Propositions are generated by the grammar

$$\phi ::= \varphi \mid \top \mid \bot \mid \phi \wedge \phi \mid \phi \to \phi \mid \phi \vee \phi \mid I \mid \phi * \phi \mid \phi \mathrel{-\!\!*} \phi$$

giving a set Prop of propositions. The connectives $\wedge$, $\to$, $\vee$, $\top$, $\bot$ stand for *additive* conjunction, implication, disjunction, truth and falsity, respectively. The connectives $*$, $\mathrel{-\!\!*}$ and I are the *multiplicative* conjunction, implication and unit, respectively.

The development of bunched logic hinges on the use of contexts Γ for formulae that are structured in a particular way. *Bunches* of propositions are generated by

$$\Gamma ::= \varnothing \mid \varnothing_* \mid \phi \mid \Gamma ; \Gamma \mid \Gamma , \Gamma .$$

The constants $\varnothing$ and $\varnothing_*$ are the additive and multiplicative units, respectively. Notice that bunches are trees with leaves labelled by propositions or units and each internal node is labelled by either the additive context former ';' or the multiplicative ','.

A *sub-bunch* of Γ is just a sub-tree such that all leaves are labelled by propositions. We write, for example, $\Gamma(\Delta)$ for a bunch containing a sub-bunch Δ. We may substitute bunches for sub-bunches. Given a bunch $\Gamma(\Delta)$, we write either $\Gamma[\Delta'/\Delta]$ or $\Gamma(\Delta')$ for the result of substituting Δ' for Δ in Γ.

We introduce a congruence relation $\equiv$ on bunches. This is generated by applying the commutative monoid axioms to each of the binary operations ';' and ',' at arbitrary depth in a bunch. The axioms ensure that the operation ';' with $\top$ defines a commutative monoid (up to $\equiv$) on the set of bunches, as does ',' with I. This relation is used to control the exchange rule for **BI**.

We will present our bunched logics in natural-deduction-style calculi. The rules for the basic system of intuitionistic **BI** are given in Figure 2. We write $\Gamma \vdash \phi$ and say that this is *derivable* when it occurs at the root of a derivation using the proof rules. The calculus has a number of important properties, including cut-elimination and the existence of known decision procedures.

Let **R** be a resource monoid. For the purposes of this subsection the preorder is not required to be discrete. Let $\mathscr{U}(\mathbf{R})$ be the collection of all upper sets of **R** (those that are upper closed with respect to the order). We write $\uparrow \mathscr{R}$ for the upwards closure of a subset

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

$$\text{(Axiom)}\ \frac{}{\phi \vdash \phi} \qquad (\Gamma \equiv \Delta)\ \frac{\Gamma \vdash \phi \quad \Delta \vdash \phi}{}\ (E)$$

$$(W)\ \frac{\Gamma(\Delta) \vdash \phi}{\Gamma(\Delta;\Delta') \vdash \phi} \qquad \frac{\Gamma(\Delta;\Delta) \vdash \phi}{\Gamma(\Delta) \vdash \phi}\ (C)$$

$$(II)\ \frac{}{\varnothing_* \vdash I} \qquad \frac{\Delta \vdash I \quad \Gamma(\varnothing_*) \vdash \phi}{\Gamma(\Delta) \vdash \phi}\ (IE)$$

$$(*I)\ \frac{\Gamma \vdash \phi \quad \Delta \vdash \psi}{\Gamma,\Delta \vdash \phi * \psi} \qquad \frac{\Delta \vdash \phi * \psi \quad \Gamma(\phi,\psi) \vdash \theta}{\Gamma(\Delta) \vdash \theta}\ (*E)$$

$$(-\!\!*I)\ \frac{\Gamma,\phi \vdash \psi}{\Gamma \vdash \phi -\!\!* \psi} \qquad \frac{\Gamma \vdash \phi \quad \Delta \vdash \phi -\!\!* \psi}{\Gamma,\Delta \vdash \psi}\ (-\!\!*E)$$

$$(\top I)\ \frac{}{\Gamma \vdash \top} \qquad \frac{\Delta \vdash \top \quad \Gamma(\varnothing) \vdash \phi}{\Gamma(\Delta) \vdash \phi}\ (\top E)$$

$$(\wedge I)\ \frac{\Gamma \vdash \phi \quad \Delta \vdash \psi}{\Gamma;\Delta \vdash \phi \wedge \psi} \qquad \frac{\Delta \vdash \phi \wedge \psi \quad \Gamma(\phi;\psi) \vdash \theta}{\Gamma(\Delta) \vdash \theta}\ (\wedge E)$$

$$(\to I)\ \frac{\Gamma;\phi \vdash \psi}{\Gamma \vdash \phi \to \psi} \qquad \frac{\Gamma \vdash \phi \quad \Delta \vdash \phi \to \psi}{\Gamma;\Delta \vdash \psi}\ (\to E)$$

$$(\vee I_i)\ \frac{\Gamma \vdash \phi_i}{\Gamma \vdash \phi_1 \vee \phi_2}\ (i = 1,2) \qquad \frac{\Delta \vdash \phi \vee \psi \quad \Gamma(\phi) \vdash \theta \quad \Gamma(\psi) \vdash \theta}{\Gamma(\Delta) \vdash \theta}\ (\vee E)$$

$$\text{(Cut)}\ \frac{\Delta \vdash \phi \quad \Gamma(\phi) \vdash \psi}{\Gamma(\Delta) \vdash \psi} \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash \phi}\ (\bot E)$$

Fig. 2. Axioms for (intuitionistic) **BI**

$\mathscr{R}$ of $\mathbf{R}$. There is a binary operation $*$ on $\mathscr{U}(\mathbf{R})$ defined by

$$\mathscr{R} * \mathscr{S} = \uparrow \{R \circ S \mid R \in \mathscr{R} \ \&\ S \in \mathscr{S} \ \&\ R \circ S \text{ is defined}\}$$

for all $\mathscr{R}, \mathscr{S} \in \mathscr{U}(\mathbf{R})$.

The logical calculus can be given a forcing semantics on resource monoids. Suppose we have a valuation $\mathscr{V} : \mathsf{Prop}_0 \longrightarrow \mathscr{U}(\mathbf{R})$ of atomic propositions. We define a satisfaction relation $\vDash \subseteq \mathbf{R} \times \mathsf{Prop}$ in Figure 3. Each valuation determines an interpretation function $[\![-]\!] : \mathsf{Prop} \longrightarrow \mathscr{U}(\mathbf{R})$ given by

$$R \in [\![\phi]\!] \quad \text{iff} \quad R \vDash \phi$$

for all $R \in \mathbf{R}$ and propositions ϕ. The interpretation of formulae extends to an interpretation of **BI**-sequents by taking

$$[\![\varnothing]\!] = [\![\top]\!] \qquad [\![\varnothing_*]\!] = [\![I]\!] \qquad [\![\phi]\!] = [\![\phi]\!] \qquad [\![\Gamma;\Delta]\!] = [\![\Gamma]\!] \cap [\![\Delta]\!] \qquad [\![\Gamma,\Delta]\!] = [\![\Gamma]\!] * [\![\Delta]\!]$$

for all sequents Γ and Δ and all formulae ϕ.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

$R \vDash \varphi$	iff $R \in \mathscr{V}(\varphi)$
$R \vDash \top$	always
$R \vDash \bot$	never
$R \vDash \phi \wedge \psi$	iff $R \vDash \phi$ and $R \vDash \psi$
$R \vDash \phi \vee \psi$	iff $R \vDash \phi$ or $R \vDash \psi$
$R \vDash \phi \to \psi$	iff $\forall S.\ R \sqsubseteq S$ and $S \vDash \phi$ implies $S \vDash \psi$
$R \vDash I$	iff $e \sqsubseteq R$
$R \vDash \phi_1 * \phi_2$	iff $\exists R_1, R_2.\ R_1 \circ R_2 \sqsubseteq R$ and $R_1 \vDash \phi_1$ and $R_2 \vDash \phi_2$
$R \vDash \phi \mathrel{-\!\!*} \psi$	iff $\forall S.\ R \circ S \downarrow$ and $S \vDash \phi$ implies $R \circ S \vDash \psi$

Fig. 3. Interpretation of **BI**

Proposition 23. The axioms of **BI** are sound with respect to the forcing semantics. That is,

$$\Gamma \vdash \phi \quad \text{implies} \quad [\![\Gamma]\!] \subseteq [\![\phi]\!]$$

holds.

An algebraic re-formulation of soundness is useful. This says that the set $\mathscr{U}(\mathbf{R})$ has a natural **BI**-algebra structure – see Pym *et al.* (2004) and Pym (2002) for more on **BI**-algebras. In particular, this uses the operation $*$ above. This construction is a mild generalisation of the construction of a quantale from a partially ordered monoid (satisfying the bifunctoriality condition). It is also an instance of Day's construction of (enriched) doubly closed categories (Day 1970; 1973). The definition of interpretation can evidently be modified to give an interpretation on the lower sets of a dual resource monoid.

We take the system **BIc** of classical **BI** to consist of classical additive connectives and intuitionistic multiplicative connectives. This system, as well as more intricate variants with classical multiplicatives, are discussed in O'Hearn and Pym (1999), Pym *et al.* (2004) and Pym (1999; 2002). We add the logical connective for negation by defining $\neg\phi$ to be $\phi \to \bot$ for all propositions ϕ. The system **BIc** is formed by adding the rule

$$\text{(RAA)} \qquad \frac{\Gamma \vdash \neg\neg\phi}{\Gamma \vdash \phi}$$

to **BI**.

In order to give a semantics, we restrict to resource monoids **R** with discrete order. That is, $R \sqsubseteq S$ if and only if $R = S$ for all $R, S \in \mathbf{R}$. Notice that the bifunctoriality

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

condition becomes vacuous in this situation. Valuations are defined as for **BI**. Note that now $\mathscr{U}(\mathbf{R}) = \mathscr{P}(\mathbf{R})$, so atomic propositions are interpreted as arbitrary subsets of **R**. It is then easy to verify that the rule (RAA) is sound.

Proposition 24. The axioms of **BIc** are sound with respect to the interpretation on resource monoids with discrete order.

The algebraic formulation of this says that $\mathscr{P}(\mathbf{R})$ is a Boolean **BI**-algebra, that is, a **BI**-algebra such that $\neg$ (as complementation) makes it a Boolean algebra.

We define the system $\mathbf{BIc}^{-I}$ to be the same as **BIc** but with the unit I and all rules involving it excised. The propositional systems **BI** and **BIc** can be extended to include first-order predication and quantifiers as in O'Hearn and Pym (1999), Pym (1999), Pym *et al.* (2004) and Pym (2002). This provides additive and multiplicative variants of both the existential and universal quantifiers.

3.2. *A modal logic*

We now present an extended Hennessy–Milner logic for **SCRPr**. The logic is a close relative of the logic **MBI** given in Pym and Tofts (2006; 2007) and Collinson *et al.* (2007). Here, we focus on the simplified language **MBIc**. The language **MBIc** is the same as **MBI** except that predication and quantifications over actions are omitted.

We assume sets Act of actions and Prop_0 of atomic propositions, and let φ range over such atomic propositions. The set Prop of propositions of **MBIc** is defined by the grammar

$$\phi ::= \varphi \mid \top \mid \bot \mid \phi \to \phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid I \mid \phi * \phi \mid \phi \mathrel{-\!\!*} \phi \mid [a]\phi \mid \langle a\rangle\phi \mid [a]_v\phi \mid \langle a\rangle_v\phi$$

where a is any action. Thus the language **MBIc** extends the language **BIc** with additive modalities $[a]$, $\langle a\rangle$ and multiplicative modalities $\langle a\rangle_v$, $[a]_v$ labelled by actions a. The language $\mathbf{MBIc}^{-I}$ omits the unit I. The additive modalities are the standard 'necessarily' and 'possibly' connectives familiar from modal logics, in particular, Hennessy–Milner logics for process algebras. As such, they implicitly use meta-theoretic quantification to make statements about reachable states. The multiplicative variants are related to multiplicative quantifications, as described in O'Hearn and Pym (1999), Pym (1999), Pym *et al.* (2004) and Pym (2002), and make statements about reachable states in the presence of additional resources. The logic is classical for additives, so we may define $\neg\phi$ to be $\phi \to \bot$. We could have defined $[a]\phi$ to be $\neg\langle a\rangle\neg\phi$. We will see from the semantics that we could also have defined $[a]_v\phi$ to be $\neg\langle a\rangle_v\neg\phi$. Examples justifying the inclusion of multiplicative modalities were included in Pym and Tofts (2006; 2007).

For any bunch Γ of formulae, we let $[a]\Gamma$ be the bunch formed by putting $[a]\phi$ for each ϕ of Γ, and adopt a similar convention for $\langle a\rangle\Gamma$, $[a]_v\Gamma$ and $\langle a\rangle_v\Gamma$. The rules of **MBIc** consist of the rules of **BIc** together with the rules presented in Figures 4 and 5. Notice that there is a new introduction rule for each of the modalities. With the exception of these, all of the new modal rules may be translated immediately into Hilbert-style tautologies.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

$$([]I)\quad \frac{\Gamma \vdash \psi}{[a]\Gamma \vdash [a]\psi} \qquad \frac{\Gamma \vdash \psi}{\langle a\rangle\Gamma \vdash \langle a\rangle\psi}\quad (\langle\rangle I)$$

$$(\neg[]\neg 1)\quad \frac{\Gamma \vdash \langle a\rangle\phi}{\Gamma \vdash \neg[a]\neg\phi} \qquad \frac{\Gamma \vdash \neg[a]\neg\phi}{\Gamma \vdash \langle a\rangle\phi}\quad (\neg[]\neg 2)$$

$$([]\top)\quad \frac{\Gamma \vdash \top}{\Gamma \vdash [a]\top} \qquad \frac{\Gamma \vdash \langle a\rangle\bot}{\Gamma \vdash \bot}\quad (\langle\rangle\bot)$$

$$([]\wedge 1)\quad \frac{\Gamma \vdash [a]\phi \wedge [a]\psi}{\Gamma \vdash [a](\phi \wedge \psi)} \qquad \frac{\Gamma \vdash [a](\phi \wedge \psi)}{\Gamma \vdash [a]\phi \wedge [a]\psi}\quad ([]\wedge 2)$$

$$(\langle\rangle\vee 1)\quad \frac{\Gamma \vdash \langle a\rangle\phi \vee \langle a\rangle\psi}{\Gamma \vdash \langle a\rangle(\phi \vee \psi)} \qquad \frac{\Gamma \vdash \langle a\rangle(\phi \vee \psi)}{\Gamma \vdash \langle a\rangle\phi \vee \langle a\rangle\psi}\quad (\langle\rangle\vee 2)$$

$$([]\wedge\langle\rangle)\quad \frac{\Gamma \vdash [a]\phi \wedge \langle a\rangle\psi}{\Gamma \vdash \langle a\rangle(\phi \wedge \psi)} \qquad \frac{\Gamma \vdash \langle a\rangle(\phi \wedge \psi)}{\Gamma \vdash \langle a\rangle\phi \wedge \langle a\rangle\psi}\quad (\langle\rangle\wedge)$$

$$(\langle 1\rangle)\quad \frac{\Gamma \vdash \langle 1\rangle\phi}{\Gamma \vdash \phi} \qquad \frac{\Gamma \vdash \phi}{\Gamma \vdash [1]\phi}\quad ([1])$$

$$(\langle 1\rangle I)\quad \frac{\Gamma \vdash I}{\Gamma \vdash \langle 1\rangle I} \qquad \frac{\Gamma \vdash \phi}{\Gamma \vdash \langle 1\rangle\phi \vee [1]\bot}\quad (\langle 1\rangle[1])$$

$$(\langle\rangle *)\quad \frac{\Gamma \vdash \langle a_1\rangle\phi_1 * \langle a_2\rangle\phi_2}{\Gamma \vdash \langle a_1 a_2\rangle(\phi_1 * \phi_2)}$$

Fig. 4. Axioms for the additive modalities of **MBIc**

3.3. *Semantics*

The mathematical structure on which we interpret **MBIc** is the set States of states generated by resources and processes. Recall that each state generates a transition structure. We define the interpretation of a formula at a state to be the interpretation of that formula at the corresponding transition structure in the ambient set of states. For the purposes of this section, we assume that $(\mathsf{Act}, \mathbf{R}, \mu, \nu)$ is fixed.

Recalling the global equivalence relation $\sim$, a set Σ of states is said to be $\sim$-*closed* if it satisfies the property

$$R, E \in \Sigma \quad \text{and} \quad E \sim F \quad \text{implies} \quad R, F \in \Sigma$$

for all states R, E and processes F. Let $\mathscr{P}(\mathsf{States})$ be the set of all $\sim$-closed sets of states. Another way to construct this is to lift $\sim$ up to the set of states via

$$R, E \sim S, F \qquad \text{iff} \qquad R = S \quad \text{and} \quad E \sim F$$

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

$$([]_v I)\quad \frac{\Gamma \vdash \psi}{[a]_v\Gamma \vdash [a]_v\psi} \qquad \frac{\Gamma \vdash \psi}{\langle a\rangle_v\Gamma \vdash \langle a\rangle_v\psi}\quad (\langle\rangle_v I)$$

$$(\neg[]_v\neg 1)\quad \frac{\Gamma \vdash \langle a\rangle_v\phi}{\Gamma \vdash \neg[a]_v\neg\phi} \qquad \frac{\Gamma \vdash \neg[a]_v\neg\phi}{\Gamma \vdash \langle a\rangle_v\phi}\quad (\neg[]_v\neg 2)$$

$$([-]_v\top)\quad \frac{\Gamma \vdash \top}{\Gamma \vdash [a]_v\top} \qquad \frac{\Gamma \vdash \langle a\rangle_v\bot}{\Gamma \vdash \bot}\quad (\langle -\rangle_v\bot)$$

$$([]_v \wedge 1)\quad \frac{\Gamma \vdash [a]_v\phi \wedge [a]_v\psi}{\Gamma \vdash [a]_v(\phi \wedge \psi)} \qquad \frac{\Gamma \vdash [a]_v(\phi \wedge \psi)}{\Gamma \vdash [a]_v\phi \wedge [a]_v\psi}\quad ([]_v \wedge 2)$$

$$([]_v \wedge \langle\rangle_v)\quad \frac{\Gamma \vdash [a]_v\phi \wedge \langle a\rangle_v\psi}{\Gamma \vdash \langle a\rangle_v(\phi \wedge \psi)} \qquad \frac{\Gamma \vdash \langle a\rangle_v(\phi \wedge \psi)}{\Gamma \vdash \langle a\rangle_v\phi \wedge \langle a\rangle_v\psi}\quad (\langle\rangle_v\wedge)$$

$$(\langle\rangle_v \vee 1)\quad \frac{\Gamma \vdash \langle a\rangle_v\phi \vee \langle a\rangle_v\psi}{\Gamma \vdash \langle a\rangle_v(\phi \vee \psi)} \qquad \frac{\Gamma \vdash \langle a\rangle_v(\phi \vee \psi)}{\Gamma \vdash \langle a\rangle_v\phi \vee \langle a\rangle_v\psi}\quad (\langle\rangle_v \vee 2)$$

$$([-][-]_v)\quad \frac{\Gamma \vdash [a]_v\phi}{\Gamma \vdash [a]\phi} \qquad \frac{\Gamma \vdash \langle a\rangle\phi}{\Gamma \vdash \langle a\rangle_v\phi}\quad (\langle -\rangle\langle -\rangle_v)$$

$$(\langle\rangle_v *)\quad \frac{\Gamma \vdash \langle a_1\rangle_v\phi * \langle a_2\rangle_v\phi_2}{\Gamma \vdash \langle a_1a_2\rangle_v(\phi_1 * \phi_2)}$$

Fig. 5. Axioms for the multiplicative modalities of **MBIc**

for all states R, E and S, F. This is clearly an equivalence relation. Furthermore, the $\sim$-closed subsets are seen to be in one–one correspondence with unions of families of equivalence classes of the relation $\sim$ on states. The set $\mathsf{CStates}$ does not, in general, have to be $\sim$-closed.

We now proceed to give an interpretation of the logical calculus on the set $\mathsf{CStates}$ of closed states. Consider the relation $\sim$ restricted to $\mathsf{CStates}$. Then we may consider the set $\mathscr{P}_\sim(\mathsf{CStates})$ of $\sim$-closed sets of closed states. A valuation is a function

$$\mathscr{V} : \mathsf{Prop}_0 \longrightarrow \mathscr{P}_\sim(\mathsf{CStates})$$

from the set of basic propositions to $\sim$-closed subsets of the set of all states. Every valuation extends in a canonical way to an interpretation for **MBIc**-formulae, for which the satisfaction relation is shown in Figure 6, and in which every process that appears is required to be an agent. A model for **MBIc** consists of the set of closed states together with such an interpretation.

Example 25. One of the most interesting new axioms of **MBIc** is $(\langle\rangle *)$, which is equivalent to a tautology

$$(\langle a_1\rangle\phi_1 * \langle a_2\rangle\phi_2) \rightarrow \langle a_1a_2\rangle(\phi_1 * \phi_2)$$

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

$$R, E \vDash \varphi \quad \text{iff} \quad R, E \in \mathscr{V}(\varphi)$$

$$R, E \vDash \bot \quad \text{never}$$

$$R, E \vDash \top \quad \text{always}$$

$$R, E \vDash \phi \wedge \psi \quad \text{iff} \quad R, E \vDash \phi \quad \text{and} \quad R, E \vDash \psi$$

$$R, E \vDash \phi \vee \psi \quad \text{iff} \quad R, E \vDash \phi \quad \text{or} \quad R, E \vDash \psi$$

$$R, E \vDash \phi \to \psi \quad \text{iff} \quad R, E \vDash \phi \quad \text{implies} \quad R, E \vDash \psi$$

$$R, E \vDash I \quad \text{iff} \quad R = e \quad \text{and} \quad E \sim 1$$

$$R, E \vDash \phi_1 * \phi_2 \quad \text{iff} \quad \exists R_1, R_2, E_1, E_2.\ R = R_1 \circ R_2 \quad \text{and} \quad E \sim E_1 \times E_2 \quad \text{and} \quad R_1, E_1 \vDash \phi_1 \quad \text{and} \quad R_2, E_2 \vDash \phi_2$$

$$R, E \vDash \phi \mathrel{-\!\!*} \psi \quad \text{iff} \quad \forall S, F.\ R \circ S \downarrow \ \&\ S, F \vDash \phi \quad \text{implies} \quad R \circ S, E \times F \vDash \psi$$

$$R, E \vDash [a]\phi \quad \text{iff} \quad \forall R', E'.\ R, E \xrightarrow{a} R', E' \quad \text{implies} \quad R', E' \vDash \phi$$

$$R, E \vDash \langle a \rangle \phi \quad \text{iff} \quad \exists R', E'.\ R, E \xrightarrow{a} R', E' \quad \text{and} \quad R', E' \vDash \phi$$

$$R, E \vDash [a]_v \phi \quad \text{iff} \quad \forall T, R', E'.\ R \circ T, E \xrightarrow{a} R', E' \quad \text{implies} \quad R', E' \vDash \phi$$

$$R, E \vDash \langle a \rangle_v \phi \quad \text{iff} \quad \exists T, R', E'.\ R \circ T, E \xrightarrow{a} R', E' \quad \text{and} \quad R', E' \vDash \phi$$

Fig. 6. Interpretation of **MBIc** on closed states

for all actions a_1, a_2 and propositions ϕ_1 and ϕ_2. This can be seen to describe an essential part of the operational behaviour of product processes as prescribed by the operational semantics: if resources can be split in such a way that they enable actions for a pair of processes, then they enable the product process. Furthermore, if each of the two sub-processes are known to step into processes with known properties ϕ_1 and ϕ_2, then the product process can step into some (product) process satisfying $\phi_1 * \phi_2$.

A careful reading of the handshaking process example in Pym and Tofts (2006; 2007) reveals that this is precisely how the logical specification for the process is constructed. In this example, there are a pair of processes

$$\begin{aligned} E_1 &= 1 : E_1 + go_{E_1} : E_1' \\ E_2 &= 1 : E_2 + go_{E_2} : E_2' \end{aligned}$$

that can evolve to a new state just when they agree on progress, and otherwise wait in the original state. The underlying resource monoid is assumed to be good and the modifications for all atomic actions are all rooted. Thus, we have a modification as

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

in Proposition 18. Let the root of $\mu(go_{E_i}, -)$ be $R_i \neq e$ for $i = 1, 2$ and suppose that $R_1 \neq R_2$. Let $R = R_1 \circ R_2$ and note that $R_1 \neq R \neq R_2$. The two processes either remain together in the initial state $R, E_1 \times E_2$ or progress to a new state via a transition $R, E_1 \times E_2 \overset{go_{E_1} go_{E_2}}{\rightarrow} R', E_1' \times E_2'$ where $R' = \mu(go_{E_1} go_{E_2}, R)$. If $\mu(a, R_i), E_i' \vDash \phi$ for $i = 1, 2$, we see that we have

$$R, E_1 \times E_2 \vDash (\langle go_{E_1} \rangle \phi_1) * (\langle go_{E_2} \rangle \phi_2)$$

and thus

$$R, E_1 \times E_2 \vDash \langle go_{E_1} go_{E_2} \rangle (\phi_1 * \phi_2).$$

The additive version of the axiom $(\langle\rangle *)$ together with the **BI** rules entail

$$\langle a_1 \rangle (\phi \mathrel{-\!\!*} \psi) \vdash (\langle a_2 \rangle \phi) \mathrel{-\!\!*} (\langle a_1 a_2 \rangle \psi).$$

Note that

$$(\langle a_1 \rangle \phi) * (\langle a_2 \rangle \psi) \vdash \langle a_1 a_2 \rangle (\phi * \phi) \text{ and } (\phi \mathrel{-\!\!*} \psi) * \phi \vdash \psi$$

are derivable. We can therefore make the derivation

$$\dfrac{\dfrac{\dfrac{\vdots}{\langle a_1 \rangle (\phi \mathrel{-\!\!*} \psi) * (\langle a_2 \rangle \phi) \vdash \langle a_1 a_2 \rangle ((\phi \mathrel{-\!\!*} \psi) * \phi)} \quad \dfrac{\dfrac{\vdots}{(\phi \mathrel{-\!\!*} \psi) * \phi \vdash \psi}}{\langle a_1 a_2 \rangle ((\phi \mathrel{-\!\!*} \psi) * \phi) \vdash \langle a_1 a_2 \rangle \psi}}{\langle a_1 \rangle (\phi \mathrel{-\!\!*} \psi), (\langle a_2 \rangle \phi) \vdash \langle a_1 a_2 \rangle \psi}}{\langle a_1 \rangle (\phi \mathrel{-\!\!*} \psi) \vdash (\langle a_2 \rangle \phi) \mathrel{-\!\!*} (\langle a_1 a_2 \rangle \psi)}$$

for any ϕ, ψ, a_1 and a_2 using the cut rule.

In the handshaking example, if $a_i = go_{E_i}$ for $i = 1, 2$, and ϕ_1 is $\phi_2 \mathrel{-\!\!*} \psi$, then whenever we combine $R_1, E_1 \vDash \langle go_{E_1} \rangle \phi_1$ with $R_2, E_2 \vDash \langle go_{E_2} \rangle \phi_2$, we get $R, E_1 \times E_2 \vDash \langle go_{E_1} go_{E_2} \rangle \psi$.

Note that the satisfaction of certain formulae at a given state makes use of states that lie outside the transition structure generated by that state. This is a critical difference between **MBIc** and most process logics.

This means that the model-checking problem for **MBIc** can be very hard, indeed, it is often only semi-decidable, depending on the properties of the underlying quadruple $(\mathbf{R}, \mathsf{Act}, \mu, \nu)$. The development of a proof system to accompany the language is therefore an important step.

We define a binary relation on closed states by

$$R, E \overset{\text{MBIc}}{\equiv} S, F \qquad \text{iff} \qquad \forall \phi.\ R, E \vDash \phi \iff S, F \vDash \phi$$

for all R, E, S, F. For any E, F, we write

$$E \overset{\text{MBIc}}{\equiv} F \qquad \text{iff} \qquad \forall R.\ R, E \overset{\text{MBIc}}{\equiv} R, F$$

holds.

The following result, which is related to the Hennessy–Milner theorem (Hennessy and Milner 1985), shows that there is a close relationship between the algebraic equivalence $\sim$ and the logical equivalence $\overset{\text{MBIc}}{\equiv}$:

Theorem 26. Let E and F be closed states. If $E \sim F$, then $E \overset{\text{MBIc}}{\equiv} F$ also holds.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

Proof. The proof is by induction on the structure of formulae. We show that for every formula ϕ, if we take any E, F, R with $E \sim F$ and $R, E \vDash \phi$, then $R, F \vDash \phi$. Since $\sim$ is symmetric, the fact that $R, F \vDash \phi$ implies $R, E \vDash \phi$ follows.

The base cases, where ϕ is one of φ, $\top$, $\bot$, are all immediate. In particular, the case for φ goes through because atomic propositions are valued as $\sim$-closed sets.

The step cases use the following induction hypothesis: for all sub-formulae ψ of ϕ, if for any E, F and R we have $E \sim F$, then $R, E \vDash \psi$ if and only if $R, F \vDash \psi$.

The cases for the connectives $\wedge$, $\vee$, $\rightarrow$ are all unsurprising. We omit the $[a]$ and $[a]_v$ cases as they are dual to the $\langle a \rangle$ and $\langle a \rangle_v$ cases, respectively. We now consider the other cases:

$\langle a \rangle$ Suppose $R, E \vDash \langle a \rangle \phi$. Then there is some E' such that $R, E \xrightarrow{a} R', E' \vDash \phi$. Since $E \sim F$, it follows that there is an F' with $R, F \xrightarrow{a} R', F'$ with $E' \sim F'$. By the induction hypothesis, we have that $R', F' \vDash \phi$. Therefore $R, F \vDash \langle a \rangle \phi$.

I Suppose $R, E \vDash I$. Then $R = e$ and $E \sim 1$. Therefore $F \sim 1$, and thus $R, F \vDash 1$.

$*$ Suppose $R, E \vDash \phi_1 * \phi_2$. Then there are R_1, R_2, E_1, E_2 with $R = R_1 \circ R_2$, $E \sim E_1 \times E_2$, $R_1, E_1 \vDash \phi_1$ and $R_2, E_2 \vDash \phi_2$. So we then have $F \sim E_1 \times E_2$ and thus $R, F \vDash \phi_1 * \phi_2$.

$-\!\!*I$ Suppose $R, E \vDash \phi -\!\!* \psi$. Consider any S, G such that $R \circ S$ is defined and $S, G \vDash \phi$ holds. Then $R \circ S, E \times G \vDash \psi$ holds. By Proposition 7, we have $E \times G \sim F \times G$ and thus $R \circ S, F \times G \vDash \psi$ by the induction hypothesis.

$\langle a \rangle_v$ Suppose $R, E \vDash \langle a \rangle_v \phi$. There are some T, R', E' such that $R \circ T$ is defined and $R \circ T, E \xrightarrow{a} R', E' \vDash \phi$. Since $E \sim F$, it follows that there is some F' with $R \circ T, F \xrightarrow{a} R', F'$ and $E' \sim F'$. By the induction hypothesis, we have $R', F' \vDash \phi$. Therefore $R, F \vDash \langle a \rangle_v \phi$. □

Note that neither of the I or $*$ cases requires the induction hypothesis. The fact that $\sim$ is a congruence is only required for the $-\!\!*$ case. There were errors in the original proof in Pym and Tofts (2006; 2007), which used the relation $\approx$ instead of $\sim$. This was corrected in Collinson *et al.* (2007). However, we do have the following proposition.

Proposition 27. Consider the $\{\top, \bot, \wedge, \vee, \rightarrow, \langle - \rangle, [-], I, *\}$-fragment of **MBIc**. Assume that all atomic propositions are valued as sets of closed states that are closed under $\approx$. Alter the I and $*$ clauses of the interpretation so that:

$$R, E \vDash I \quad \text{iff} \quad R, E \approx e, 1$$

$$R, E \vDash \phi_1 * \phi_2 \quad \text{iff} \quad \exists R_1, R_2, E_1, E_2.\ R = R_1 \circ R_2 \ \text{ and } \ R, E \approx R, E_1 \times E_2.$$

The following version of Theorem 26 then holds: if $R, E \approx R, F$, then $R, E \overset{\text{MBIc}}{\equiv} R, F$ for all resources R and processes E and F.

Proof. The proof is essentially as before. We suppose that $R, E \approx R, F$ and show, by induction on the structure of ϕ, that if $R, E \vDash \phi$ then $R, F \vDash \phi$. The I and $*$ cases only require the fact that $\approx$ is an equivalence relation. The other cases then hold for the standard reasons for the usual interpretation of a classical modal logic. □

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

Theorem 26 remains true for $\sim$ and with atomic predicates and additive and multiplicative quantifiers added to **MBIc**, as in Pym and Tofts (2006; 2007) and Collinson *et al.* (2007) – see also Section 3.5 below.

Theorem 26 shows that the set of closed states satisfying any formula is $\sim$-closed.

Corollary 28. Every interpretation yields a unique function

$$[\![-]\!] : \mathsf{Prop} \longrightarrow \mathscr{P}_{\sim}(\mathsf{CStates})$$

with

$$R, E \in [\![\phi]\!] \qquad \text{iff} \qquad R, E \vDash \phi$$

for all closed states R, E and **MBIc**-propositions ϕ.

The sets States and CStates have monoidal structure that the interpretation is critically dependent upon. This is easily shown using the algebraic properties of $\sim$ that we have already determined.

Proposition 29. The set States is a resource monoid with the equality given by $\sim$. The composition is defined by the Kleene equality:

$$(R, E) \times (S, F) \simeq (R \circ S, E \times F)$$

for all (R, E) and (S, F). Note that this expression is defined just when $R \circ S$ is defined. The unit is $(e, 1)$. The set CStates is a resource monoid with the same structure.

We extend the monoid on CStates to a monoid $*$ with unit I on $\sim$-closed sets of CStates by taking

$$I = \{(e, E) \mid E \sim 1\}$$

$$\Sigma_1 * \Sigma_2 = \{(R, E) \mid \exists R_1, R_2, E_1, E_2.\ R = R_1 \circ R_2 \text{ and } E \sim E_1 \times E_2 \text{ and } R_1, E_1 \in \Sigma_1 \text{ and } R_2, E_2 \in \Sigma_2\}$$

for any two sets of closed states Σ_1 and Σ_2. The interpretation extends to an interpretation of bunches and judgements following the pattern used for the semantics of **BIc**, but now using $\sim$-closed subsets of CStates in place of sets of resources.

Lemma 30. If $[\![\Delta]\!] \subseteq [\![\Delta']\!]$, then $[\![\Gamma(\Delta)]\!] \subseteq [\![\Gamma(\Delta')]\!]$ for any Γ.

The proof of this monotonicity property is by induction on the structure of Γ and uses the observation that both the intersection and $*$ operations are monotonic. In fact, they both satisfy the bifunctoriality condition (1).

Lemma 31. We have the following simple results:

$$[\![\phi]\!] = [\![\phi]\!] * [\![I]\!] \qquad \text{and} \qquad [\![\phi]\!] * [\![\phi \mathrel{-\!\!*} \psi]\!] \subseteq [\![\psi]\!]$$

for all ϕ and ψ.

Proof. The proof is by unfolding the definitions and then applying Theorem 26 and Lemma 9. The proof of the first rests upon the simple-extension property for transitions since it requires the result $E \sim E \times 1$ for all agents E. □

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

Theorem 32. The calculus **MBIc** is sound on the model above. That is,

$$\Gamma \vdash \psi \quad \text{implies} \quad [\![\Gamma]\!] \subseteq [\![\psi]\!]$$

holds, for all Γ, ψ.

Proof. The proof is by induction on the derivation of the judgement $\Gamma \vdash \psi$. This amounts to a case analysis on the final rule of the derivation. We omit the cases for the introduction and elimination rules of $\top$, $\bot$, $\wedge$, $\vee$, $\to$ as they are rather standard. The cases $[-]$ and $[-]_v$ are omitted as they are dual to the $\langle - \rangle$ and $\langle - \rangle_v$ cases, respectively.

II This case is trivial since $[\![\varnothing_*]\!] = I$.

IE The induction hypothesis means that $[\![\Delta]\!] \subseteq [\![I]\!]$ and $[\![\Gamma(\varnothing_*)]\!] \subseteq [\![\phi]\!]$. Now $[\![I]\!] = [\![\varnothing_*]\!]$, so by Lemma 30, $[\![\Gamma(\Delta)]\!] \subseteq [\![\Gamma(\varnothing_*)]\!]$, and thus $[\![\Gamma(\Delta)]\!] \subseteq [\![\phi]\!]$.

$*I$ We have $[\![\Gamma]\!] \subseteq [\![\phi]\!]$ and $[\![\Delta]\!] \subseteq [\![\psi]\!]$. Then $[\![\Gamma, \Delta]\!] = [\![\Gamma]\!] * [\![\Delta]\!] \subseteq [\![\phi]\!] * [\![\psi]\!] = [\![\phi * \psi]\!]$ using the monotonicity properties of $*$.

$*E$ We have $[\![\Delta]\!] \subseteq [\![\phi * \psi]\!] = [\![\phi, \psi]\!]$ and $[\![\Gamma(\phi, \psi)]\!] \subseteq [\![\theta]\!]$. Then $[\![\Gamma(\Delta)]\!] \subseteq [\![\theta]\!]$ by Lemma 30.

$-\!\!*I$ We have $[\![\Gamma, \phi]\!] \subseteq [\![\psi]\!]$. Now suppose $R, E \in [\![\Gamma]\!]$. Consider any closed state S, F such that $R \circ S \downarrow$ and $S, F \vDash \phi$. By the definitions of satisfaction and interpretation, we have $R \circ S, E \times F \in [\![\Gamma, \phi]\!]$. Therefore $R \circ S, E \times F \in [\![\psi]\!]$, and thus $R \circ S, E \times F \vDash \psi$. It follows that $R, E \in [\![\phi \mathrel{-\!\!*} \psi]\!]$. Therefore $[\![\Gamma]\!] \subseteq [\![\phi \mathrel{-\!\!*} \psi]\!]$ holds.

$-\!\!*E$ The induction hypothesis gives $[\![\Gamma]\!] \subseteq [\![\phi]\!]$ and $[\![\Delta]\!] \subseteq [\![\phi \mathrel{-\!\!*} \psi]\!]$. Since $*$ is bifunctorial, we have $[\![\Gamma, \Delta]\!] \subseteq [\![\phi]\!] * [\![\phi \mathrel{-\!\!*} \psi]\!]$. Applying Lemma 31, we get $[\![\Gamma, \Delta]\!] \subseteq [\![\psi]\!]$.

$\langle\rangle*$ Suppose $R, E \vDash \langle a_1 \rangle \phi_1 * \langle a_2 \rangle \phi_2$. Then there are R_1, R_2, E_1, E_2 such that $R = R_1 \circ R_2$, $E \sim E_1 \times E_2$, $R_1, E_1 \vDash \langle a_1 \rangle \phi_1$ and $R_2, E_2 \vDash \langle a_2 \rangle \phi_2$ hold. Then there are R_1' R_2', E_1', E_2' such that $R_1, E_1 \xrightarrow{a_1} R_1', E_1'$, $R_2, E_2 \xrightarrow{a_2} R_2', E_2'$ and $R_1', E_1' \vDash \phi_1$ and $R_2', E_2' \vDash \phi_2$. We can then derive $R, E_1 \times E_2 \xrightarrow{a_1 a_2} R', E_1' \times E_2'$, where $R' = R_1' \circ R_2'$. Clearly, $R', E_1' \times E_2' \vDash \phi_1 * \phi_2$ holds, and therefore so does $R, E_1 \times E_2 \vDash \langle a_1 a_2 \rangle (\phi_1 * \phi_2)$. Since $E \sim E_1 \times E_2$, we have $R, E \vDash \langle a_1 a_2 \rangle (\phi_1 * \phi_2)$, using Theorem 26. Thus, if $[\![\Gamma]\!] \subseteq [\![\langle a_1 \rangle \phi_1 * \langle a_2 \rangle \phi_2]\!]$, then $[\![\Gamma]\!] \subseteq [\![\langle a_1 a_2 \rangle (\phi_1 * \phi_2)]\!]$.

E The structural rule of equivalence makes use of the relation $\equiv$ between bunches. Proving the soundness of this makes essential use of the first result in Lemma 31.

We omit the proofs of the other rules. They are all quite straightforward consequences of the definitions and results we have developed above. □

Notice that this soundness relies upon Theorem 26, the algebraic properties of Lemma 9 and the simple-extension property for transitions. For the process calculus **SCRP** (as opposed to **SCRPr**), the logic $\mathbf{MBIc}^{-I}$ is sound under this interpretation (but **MBIc** is not).

Corollary 33. If $\varnothing \vdash \phi$, then $R, E \vDash \phi$ for all closed states R, E.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

The fact that $R, E \in [\![\varnothing_*]\!]$ entails $R = e$ and $E \sim 1$ means that we are more interested in the additive theorems (those of the form $\varnothing \vdash \phi$) than in the multiplicative theorems ($\varnothing_* \vdash \phi$).

We can give an algebraic restatement of the soundness result, namely, that the set $\mathscr{R}(\mathsf{CStates})$ is naturally equipped with the structure of a **BIc**-algebra together with operators for additive and multiplicative modalities. This all follows from the fact that CStates is a resource monoid and the fact that $\sim$ is contained in the usual bisimulation relation on states familiar from modal logic (Popkorn 1994).

3.4. *Characterisation of the logical equivalence*

We have shown above that the global simulation $\sim$ on states is contained in both the logical (semantic) equivalence $\overset{\text{MBIc}}{\equiv}$ and the local simulation $\approx$. It is not always the case that the relation $\approx$ on processes is contained in the relation $\overset{\text{MBIc}}{\equiv}$ on processes. The following counterexample shows that the relation $\approx$ on states is not contained in $\overset{\text{MBIc}}{\equiv}$ on states.

Example 34. Consider the resource monoid $\mathbf{R} = (\mathbb{N} \cup \{\infty\}, \circ, 0, =)$ with

$$m \circ n = \begin{cases} m + n & \text{if } m, n \in \mathbb{N} \\ \infty & \text{if } (m = 0 \text{ and } n = \infty) \text{ or } (m = \infty \text{ and } n = 0) \\ \uparrow & \text{otherwise.} \end{cases}$$

Take the action monoid $Act = \{b^p \mid p \in \mathbb{N}\}$ generated freely from the atomic action b. In particular, we write $1 = b^0$.

The following defines a modification:

$$\mu(b^p, n) = \begin{cases} n & \text{if } n \in \mathbb{N} \text{ and } p = 0 \\ \uparrow & \text{if } n \in \mathbb{N} \text{ and } p \neq 0 \\ \infty & \text{if } n = \infty \text{ and } p = 0 \\ 0 & \text{if } n = \infty \text{ and } p \neq 0. \end{cases}$$

Consider the processes E and F defined by

$$E \;=\; 1 : E + b : E \qquad\qquad F \;=\; 1 : F.$$

For any $n \in \mathbb{N}$, the only transition of n, E is $n, E \xrightarrow{1} n, E$, and the only transition of n, F is $n, F \xrightarrow{1} n, F$, since $\mu(1, n) = n$ and $\mu(b, n) \uparrow$. Therefore, $n, E \approx n, F$ for any $n \in \mathbb{N}$.

Note that ∞, E and ∞, F have distinct operational behaviour since $\infty, E \xrightarrow{b} 0, E$, but there is no b-transition starting from ∞, F. Therefore, $\infty, E \not\approx \infty, F$.

Consider the atomic proposition ϕ valued such that

$$n, E' \vDash \phi \qquad \text{iff} \qquad n = \infty \quad \text{and} \quad E' \sim 1$$

for all n and E'.

Consider any n and E' such that $n, E' \vDash \phi$, so that $n = \infty$ and $E' \sim 1$. Then

$$\frac{\infty, E \xrightarrow{b} 0, E \qquad 0, E' \xrightarrow{1} 0, E'}{\infty \circ 0, E \times E' \xrightarrow{b} 0 \circ 0, E \times E'}$$

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

since $\mu(b,\infty) = 0$. Now $\infty, E \times E' \xrightarrow{b} 0, E \times E'$ and $0, E \times E' \vDash \top$, so $0 \circ \infty, E \times E' \vDash \langle b \rangle \top$. Therefore, $0, E \vDash \phi \mathrel{-\!\!*} \langle b \rangle \top$, since the above argument holds for arbitrary n and E'. On the other hand, $0, F \nvDash \phi \mathrel{-\!\!*} \langle b \rangle \top$ since $\infty, 1 \vDash \phi$ but $0 \circ \infty, F \times 1$ makes no b-transition.

Therefore,

$$0, E \approx 0, F \qquad \text{and} \qquad 0, E \overset{\text{MBIc}}{\not\equiv} 0, F$$

both hold.

For standard process algebras like SCCS there is a partial converse to Theorem 26, which says that, under certain conditions, any two logically equivalent processes are also $\approx$-equivalent.

We define a state R, E to be *image finite* if it has finitely many immediate derivatives. We define an agent E to be image finite if R, E is image finite for all R. We define a process E with all free variables amongst the n-tuple X to be image finite if $E[\mathsf{G}/\mathsf{X}]$ is image finite for all n-tuples of agents G. We then have the following result.

Theorem 35. If $R, E \overset{\text{MBIc}}{\equiv} R, F$ for any image-finite processes E and F and any resource R, then $R, E \approx R, F$ holds. Consequently, if $E \overset{\text{MBIc}}{\equiv} F$, then $E \approx F$ holds.

Proof. Note that if the theorem is true, then $\overset{\text{MBIc}}{\equiv}$ is contained in $\approx$ on states, and thus $\overset{\text{MBIc}}{\equiv}$ must satisfy the closure conditions defining $\approx$.

Suppose in order to show a contradiction that the theorem is false. Then there must be some states R, E and R, F with $R, E \overset{\text{MBIc}}{\equiv} R, F$ and, without loss of generality, some transition $R, E \xrightarrow{a} \mu(a, R), E'$ for some E' and some a such that there is no F' with both $R, F \xrightarrow{a} \mu(a, R), F'$ and $\mu(a, R), E' \overset{\text{MBIc}}{\equiv} \mu(a, R), F'$.

Let $\mathscr{F} = \{F' \mid R, F \xrightarrow{a} \mu(a, R), F'\}$. If $\mathscr{F}$ is empty, then $R, E \vDash \langle a \rangle \top$ and $R, F \nvDash \langle a \rangle \top$, which contradicts $R, E \overset{\text{MBIc}}{\equiv} R, F$. Therefore $\mathscr{F}$ must be non-empty. Since F is image finite, we may enumerate the elements of $\mathscr{F}$ as $F_1, \ldots, F_n$ for some $n \geqslant 1$. Furthermore, since $\mu(a, R), E' \overset{\text{MBIc}}{\not\equiv} \mu(a, R), F_i$ for every $F_i \in \mathscr{F}$ and **MBIc** has classical negation, for each $1 \leqslant i \leqslant n$ there is some ϕ_i such that $\mu(a, R), E' \vDash \phi_i$ and $\mu(a, R), F_i \nvDash \phi_i$. But then $R, E \vDash \langle a \rangle (\phi_1 \wedge \ldots \wedge \phi_n)$ and $R, F \nvDash \langle a \rangle (\phi_1 \wedge \ldots \wedge \phi_n)$, which contradicts $R, E \overset{\text{MBIc}}{\equiv} R, F$, so $\mathscr{F}$ cannot be non-empty either. □

The **SCRP**-version of this result was shown in Pym and Tofts (2006). The main work in the proof is done by the presence of the additive diamond modality, which allows us to distinguish processes that make different transitions. This is a general fact of modal logic – see Popkorn (1994) for a detailed explanation. Indeed, the proof will work for any fragment of **MBIc** including $\langle\rangle$, $\wedge$ and $\top$.

It does not seem that an analogous result can be produced for $\sim$, even with the multiplicative connectives. In particular, an equivalence $E \sim F$ makes comparisons of states S, E' where E' is the process component of a derivative R', E' of some state R, E, with $S \neq R'$. However, the multiplicative diamond only gives access to states with resource components that are formed as composites of some resource with the resource component of derivatives. In general, not all resources can be realised as such composites. The connectives $\mathrel{-\!\!*}$ and $*$ also do not seem to be of any help here.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

We find ourselves in the situation of having Theorem 26 stated using the relation $\sim$, but no converse. This is somewhat unsatisfactory. Ideally, one would wish to have a single bisimulation relation that matched perfectly with the logical equivalence.

The relation $\approx$ on states seems like the natural way to compare the operational behaviour of states and is also intimately related to the soundness of the classical modal connectives. We have seen, however, that it is not always a congruence. This means that it cannot be used to give a logical interpretation of **MBIc** (along the lines of Proposition 27) that supports the connective $-\!\!*$ (it also does not support $\langle\rangle_v$).

The failure of congruence for $\approx$ on states is a consequence of the form of the operational rule for synchronous product, and the fact that resource composition is not injective. This also holds for the relation $\approx$ on processes, which may further fail to be closed under transitions on states: there exists E, E', F, R and R', with $E \approx F$ and $R, E \xrightarrow{a} R', E'$ but no F' with $R, F \xrightarrow{a} R', F'$ and $E' \approx F'$. Hence this relation does not give a version of Theorem 26 featuring the additive or multiplicative modalities.

The relation $\sim$ is a conservative solution to the failure of both notions of $\approx$ above. The use of universal quantification across resources and the fact that it is closed under transitions guarantee that it is a congruence and that Theorem 26 and Theorem 32 hold.

The logic **MBIc** is concerned with composition and decomposition of states and resources as well as operational behaviour. Thus one should perhaps expect that a bisimulation relation that matches $\overset{\mathbf{MBIc}}{\equiv}$ should compare more than just the operational behaviour of states – it should also compare composition and decomposition of states and resources.

There is a line of work that has developed methods for designing labelled transition systems for process calculi that satisfy general forms of bisimulation (Sewell 1998; Leifer and Milner 2000; Sassone and Sobociński 2003). We do not know if such methods can be used to redesign the labelled transition system of **SCRP** in such a way as to make $\approx$ better behaved, or to find a suitable alternative to $\sim$.

3.5. *Quantification*

The above system is purely propositional. In contrast, Pym and Tofts (2006; 2007) and Collinson *et al.* (2007) showed that quantification can be extremely useful: in particular, for describing the resource-hiding restriction mechanism of **SCRP**. In this section we consider an extension, **MBIq**, of our previous logical system, **MBIc**, with such quantification.

It turns out that what we need for the discussion of hiding is quantification over an action. Thus we assume a countable set ActVar of *action variables*, ranged over by x, and a constant symbol a for each action a of **SCRPr**. Let $\mathsf{A} = \mathsf{ActVar} \cup \mathsf{Act}$ with a ranging over this set. We assume a given set of function symbols on actions, each with some chosen arity. The *terms* t of the language are then formed in the standard way (variables and constants are terms, functions applied to terms are terms). We assume a given set of *relations* on the set of actions, each with a given arity. We assume the equality relation $=$ between terms to be included in this set. Atomic formulae φ consist of all instances of relations, that is, if p is a relation symbol of arity n and $t_1, \ldots, t_n$ are terms, then $p(t_1, \ldots, t_n)$

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

$$R, E \vDash p(t_1, \ldots, t_n)\eta \text{ iff } (t_1\eta, \ldots, t_n\eta, (R, E)) \in \mathscr{V}(p)$$

$$R, E \vDash (\exists x.\phi)\eta \text{ iff } \exists a \in \mathsf{Act}.\ R, E \vDash \phi[a/x]\eta$$

$$R, E \vDash (\forall x.\phi)\eta \text{ iff } \forall a \in \mathsf{Act}.\ R, E \vDash \phi[a/x]\eta$$

$$R, E \vDash (\exists_v x.\phi)\eta \text{ iff } \exists (S, F) \in \mathsf{CStates}.\ \exists a \in \mathsf{Act}.\ R, E \sim R, \nu S.F \text{ and } R \circ S \downarrow \text{ and } \mu(a, S) \downarrow \text{ and } R \circ S, F \vDash \phi[a/x]\eta$$

$$R, E \vDash (\forall_v x.\phi)\eta \text{ iff } \forall (S, F) \in \mathsf{CStates}.\forall a \in \mathsf{Act}.\ R, E \sim R, \nu S.F \text{ and } R \circ S \downarrow \text{ and } \mu(a, S) \downarrow \text{ implies } R \circ S, F \vDash \phi[a/x]\eta$$

Fig. 7. Interpretation of **MBIq**

is an atomic formula. The formulae of the language **MBIq** are then as follows:

$$\phi ::= \varphi \mid \top \mid \bot \mid \phi \to \phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid I \mid \phi * \phi \mid \phi \mathrel{-\!\!*} \phi$$

$$\mid [\mathsf{a}]\phi \mid \langle \mathsf{a} \rangle \phi \mid [\mathsf{a}]_v \phi \mid \langle \mathsf{a} \rangle_v \phi \mid \exists x.\phi \mid \forall x.\phi \mid \exists_v x.\phi \mid \forall_v x.\phi.$$

Notice that we now have modalities $\langle x \rangle$, $[x]$, $\langle x \rangle_v$ and $[x]_v$ labelled by variables (in this case x) as well as action constants. The additive quantifiers $\exists$, $\forall$ and the multiplicative quantifiers $\exists_v$, $\forall_v$ bind free action variables (in the usual way). The *sentences* are just the formulae without free variables. For any formula ϕ, let $\phi[t_1/x_n, \ldots, t_n/x_n]$ be the formula formed by replacing each occurrence of each variable x_i by the term t_i.

A valuation $\mathscr{V}$ for the language above is fixed by choosing a relation $\mathscr{V}(p) \subseteq \mathsf{Act}^n \times \mathsf{CStates}$ for each relation symbol p of arity n and an n-ary function on Act for each n-ary function symbol. In particular, $\mathscr{V}(=) = \{(a, a, (R, E)) \mid a \in \mathsf{Act}, (R, E) \in \mathsf{CStates}\}$. Each set $\mathscr{V}(p)$ must be closed under the relation $\sim$. An *assignment* η is a function from ActVar to Act. For any η, let $\eta[a/x]$ be the assignment that is identical to η except that $\eta(x) = a$. Constants are interpreted as themselves at any assignment. A variable x is interpreted as $\eta(x)$ at any assignment η. Compound terms are interpreted at an assignment by applying the interpretation of the outermost function symbol to the interpretation of sub-terms: thus all terms denote actions. A valuation is then extended to an interpretation of formulae as in Figure 7 with the understanding that the interpretation of all other formulae follows the pattern in Figure 6. In particular, the interpretations of $\langle x \rangle$, $[x]$, $\langle x \rangle_v$, $[x]_v$ follow from those of $\langle a \rangle$, $[a]$, $\langle a \rangle_v$, $[a]_v$, respectively, by replacing all occurrences of a by x.

There are a number of special cases of the above set-up that are particularly important. The first of these is the case where there are no function symbols, so the only terms are the variables and (constant) actions. A second recovers atomic propositions that are independent of action (as in **MBIc**) by including relations of arity 0 (note that these are distinct from action constants). Notice that in this case quantification is only over actions that occur as labels of modalities.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

The situation in Pym and Tofts (2006; 2007) and Collinson *et al.* (2007) follows the first of the special cases (no function symbols). In addition, only a special form of relation is allowed. These are defined (with a slight change of notation) to be those susceptible to an interpretation

$$R, E \vDash p(a_1, \ldots, a_n) \;\text{ iff }\; \forall 1 \leqslant i \leqslant n.\ \mu(a_i, R)\downarrow \;\text{ and }\; [\![p]\!](R, \ldots, R)$$

where $[\![p]\!] \subseteq \mathbf{R}^n$ is an n-ary relation on resources associated with the relation symbol p. For a relationship $R, E \vDash \phi$ for a formula ϕ of the form $\exists x.\langle x\rangle\phi$ or $\exists x.p(x)$, any witness a for x will clearly satisfy $\mu(a, R)\downarrow$. Similarly, for formulae of the form $\forall x.\langle x\rangle\phi$ we only need to verify that $\phi[a/x]$ whenever $\mu(a, R)$ is defined. A slightly different formulation of the additive quantifiers was presented in Pym and Tofts (2006; 2007) and Collinson *et al.* (2007), and these conditions $\mu(a, R)\downarrow$ were explicitly included. We have preferred the slightly more general version here. This is likely to give cleaner proof rules.

The multiplicative quantifier $\exists_v$ is intended to characterise hiding in the same sense that $*$ characterises synchronous product. Examples of the use of multiplicative quantification are given in Pym and Tofts (2006; 2007).

Example 36. The privacy example contained in Pym and Tofts (2007) can, in fact, be illustrated through the combination of the two special cases above. This example is a continuation of Example 25. The resources used by the evolving state $R_1 \circ R_2, E_1 \times E_2$ may be hidden to form some new state

$$e, v(R_1 \circ R_2).(E_1 \times E_2)$$

in which the resources are no longer externally visible. If this state evolves (because it meets the side conditions on the transition rule for hiding processes), it does so in the same way as before, apart from two differences:

1 The evolution of $R_1 \circ R_2$ is no longer externally invisible.
2 The state now evolves along the action $v(R_1 \circ R_2).a$ so that a itself may not be externally observable.

In the case of the choice of v from equation (3), only the atoms of a that do not use $R_1 \circ R_2$ are externally visible.

Suppose the state $e, v(R_1 \circ R_2).(E_1 \times E_2)$ does evolve. Then we have the satisfaction relation

$$e, v(R_1 \circ R_2).(E_1 \times E_2) \vDash \exists_v x.\langle x\rangle(\phi_1 * \phi_2)$$

since $R_1 \circ R_2, E_1 \times E_2 \vDash \langle go_{E_1} go_{E_2}\rangle(\phi_1 * \phi_2)$ holds. Furthermore, the fact that $\exists_v$ is used forces the process to be a hiding (resource restriction), at least up to global bisimulation, and the action x (instantiated by $go_{E_1} go_{E_2}$) to be such that the hidden resource enables it to act.

We write

$$R, E \overset{\mathbf{MBIq}}{\equiv} R, F \;\text{ iff }\; \forall \phi\ .R, E \vDash \phi \iff R, F \vDash \phi$$

for any closed states R, E and R, F, and we write $E \overset{\mathbf{MBIq}}{\equiv} F$ whenever $R, E \overset{\mathbf{MBIq}}{\equiv} R, F$ for all R. The appropriate extension of Theorem 26 holds.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

Theorem 37. Let E and F be agents. If $E \sim F$, then $E \overset{\mathbf{MBIq}}{\equiv} F$ also holds.

Proof. The proof is an extension of the induction given for Theorem 26. The new clauses in the proof are almost trivial given the interpretation above. The valuations of atoms are assumed to be closed under $\sim$. The induction steps at the additive quantifiers are straightforward, and the steps for the multiplicative quantifiers only use the fact that $\sim$ is an equivalence relation. □

We have not considered any proof rules for the quantifiers of **MBIq**. It seems that the additives should satisfy the standard rules for first-order quantification and that these should be susceptible to the usual semantics using indexed categories following Lawvere (1969). How to do this for the multiplicatives and how to produce an appropriate extension of Theorem 32 is completely open.

It may well be the case that further enrichments of the calculus with, for example, a resource sort, function symbols for partial functions and equality would prove fruitful. Clearly, they would approximate more closely the level of detail involved in the satisfaction relation $\models$, in particular, allowing us to deal directly with properties of modifications within the logic.

4. Ordered SCRP and intuitionistic MBI

None of the work on members of the **SCRP** and **MBI** families of calculi has so far made any use of the order on resource monoids. In this section we will develop calculi that are sensitive to the order. The process calculus **OSCRP** deals with actions that are performed just when they have sufficient resources. A special version of such a calculus has already been considered in Pym and Tofts (2006) using an *enabling function* $\rho : \mathsf{Act} \longrightarrow \mathbf{R}$ to specify the minimum resources required for an action to fire. This kind of calculus was suitable for most of the modelling situations under consideration but was difficult to reconcile with a Hennessy–Milner logic with classical modalities. We now show that the appropriate logic for reasoning about **OSCRP** is a modal logic with an intuitionistic proof system and semantics. Again we consider only the propositional part, and call the new logic **MBIi**.

The use of order in both the process calculus and the logic has considerable practical advantages. For example, in a system that automatically generates the transition system associated with a resource-process state, the computationally hard part can be determining the evolution of resources under an arbitrary modification. The use of an order can substantially simplify these calculations. In a similar way, a model-checker that attempts automatically to verify assertions of **MBI** against states must, in general, deal with unbounded searches across infinite resource spaces. Suitable structuring using the order and modification can bound this search and thus yield a model-checker with better termination properties.

We begin with a special resource monoid $\mathbf{R} = (\mathbf{R}, \circ, e, \sqsubseteq)$ and an action monoid Act. A modification μ is a partial function satisfying the coherence conditions (for **SCRPr**)

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

previously stated, but we suppose that it also satisfies both of the following monotonicity conditions:

1 if $\mu(a, R)\downarrow$ and $R \sqsubseteq S$, then $\mu(a, S)\downarrow$ and $\mu(a, R) \sqsubseteq \mu(a, S)$;
2 if $\mu(a, R \circ S)$ and $\mu(\nu S.a, R) \circ S'$ are both defined with $\mu(a, R \circ S) = \mu(\nu S.a, R) \circ S'$ and $R \sqsubseteq T$, then $\mu(a, T \circ S)$ and $\mu(\nu S.a, T) \circ S'$ are defined and $\mu(a, T \circ S) = \mu(\nu S.a, T) \circ S'$

for all actions a and resources R, S, S', T.

It is easy to verify that Lemma 3 concerning the extension of resources and modifications holds in this new setting. An additional observation about the piggybacking relation and the order is needed, the proof of which is immediate.

Lemma 38. If the resource monoid is special and $S \circledcirc R$ and $R \sqsubseteq T$ hold, then $S \circledcirc T$ holds.

The process terms are precisely the same as for **SCRPr**, as are the operational rules, with the exception of the product, which becomes

$$\frac{R, E \xrightarrow{a} R', E' \qquad S, F \xrightarrow{b} S', F'}{T, E \times F \xrightarrow{ab} \mu(ab, T), E' \times F'} \qquad (R \circ S \sqsubseteq T)$$

for all appropriate a, b, E, E', F, F', R, R', S, S', T.

As before, the form of the rules means that the only resource that appears in the target of a transition is the modification of the resource in the source of that transition. That is, Lemma 2 holds in this setting. The rule for prefix and the monotonicity conditions on μ mean that if the state $R, a : E$ makes a transition and $R \sqsubseteq S$, then so does $S, a : E$. In fact, we have the following *order-extension property* for transitions.

Lemma 39. If $R, E \xrightarrow{a} \mu(a, R), E'$ and $R \sqsubseteq R'$, then $R', E \xrightarrow{a} \mu(a, R'), E'$ is also derivable.

Proof. The proof is much as one would expect, that is, by induction on the derivation of the process term E. The prefix case holds for the reasons noted above. The sum case is straightforward. The product case is taken care of by the order in the side condition. The hiding case follows because of the new condition on modifications regarding hiding actions and the monotonicity condition for the predicate $\circledcirc$ noted in Lemma 38. □

The simple-extension property for transitions, Lemma 4, holds in this new setting, and the proof is much as before. The product case now makes use of the bifunctoriality condition on the resource monoid and the hiding case makes use of the predicate $\circledcirc$.

The global bisimulation relation $\sim$ is defined precisely as before. That is, it takes no account of the order. On the other hand, if we had wished to work with the local variant, we would have had to place some compatibility constraints between it and the order. The global bisimulation is shown to be an equivalence relation and a congruence as before (Lemma 7), with only minor alterations to the product clause. The simple algebraic properties of Lemma 9 continue to hold: in particular, the clause that says that $\mathbf{1}$ is a unit for $\times$ makes use of Proposition 4 and Lemma 39, and the associativity of $\times$ makes use of the new monotonicity condition on composition.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

$$R, E \vDash \varphi \quad \text{iff} \quad R, E \in \mathscr{V}(\varphi)$$

$$R, E \vDash \phi \to \psi \text{ iff } \forall S.\ R \sqsubseteq S \quad \text{and} \quad S, E \vDash \phi \quad \text{implies} \quad S, E \vDash \psi$$

$$R, E \vDash I \text{ iff } e \sqsubseteq R \quad \text{and} \quad E \sim 1$$

$$R, E \vDash \phi_1 * \phi_2 \text{ iff } \exists R_1, R_2, E_1, E_2.\ R_1 \circ R_2 \sqsubseteq R \quad \text{and} \quad E \sim E_1 \times E_2 \quad \text{and} \quad R_1, E_1 \vDash \phi_1 \quad \text{and} \quad R_2, E_2 \vDash \phi_2$$

$$R, E \vDash [a]\phi \text{ iff } \forall S, S', E'.\ R \sqsubseteq S \ \&\ S, E \xrightarrow{a} S', E' \quad \text{implies} \quad S', E' \vDash \phi$$

$$R, E \vDash \langle a \rangle \phi \text{ iff } \forall S.\ R \sqsubseteq S \quad \text{implies } \exists S', E'.\ S, E \xrightarrow{a} S', E' \quad \text{and} \quad S', E' \vDash \phi$$

$$R, E \vDash [a]_v \phi \text{ iff } \forall S, T, S', E'.\ R \sqsubseteq S \ \&\ S \circ T, E \xrightarrow{a} S', E' \quad \text{implies} \quad S', E' \vDash \phi$$

$$R, E \vDash \langle a \rangle_v \phi \text{ iff } \forall S.\ R \sqsubseteq S \quad \text{implies} \quad \exists T, S', E'.\ S \circ T, E \xrightarrow{a} S', E' \quad \text{and} \quad S', E' \vDash \phi$$

Fig. 8. Interpretation of MBIi

We introduce a logic **MBIi** of intuitionistic modal propositional **MBI**. This has the same connectives as **MBIc** and all of the same rules except for (RAA), $(\neg[]\neg 2)$, $(\langle\rangle \vee 2)$, $(\langle 1\rangle[1])$, $(\langle\rangle_v I)$, $(\neg[]_v\neg 2)$, $(\langle\rangle_v \vee 2)$, $(\langle\rangle\langle\rangle_v)$, which are omitted.

4.1. *Interpretation*

We define a preorder on states by

$$R, E \sqsubseteq S, F \qquad \text{iff} \qquad R \sqsubseteq S \quad \text{and} \quad E = F$$

for all E, F, R, S, where $=$ is the identity on the syntax of processes. Let the set of all upper sets amongst the states be $\Upsilon(\mathsf{States})$, and the set of all $\sim$-closed upper sets be $\Upsilon_\sim(\mathsf{States})$.

A valuation of atomic propositions is taken to be a map

$$\mathscr{V} : \mathsf{Prop}_0 \longrightarrow \Upsilon_\sim(\mathsf{CStates})$$

from the set of atomic propositions Prop_0 to the $\sim$-closed upper sets of closed states. For any given valuation $\mathscr{V}$ of the atomic propositions, the language **MBIi** is given an interpretation on closed states as in Figure 8. This makes use of the order on the resource monoid. We omit the interpretation of the $\wedge$, $\vee$ and $-\!\!*$ connectives as they remain the same as in Figure 6.

The recursive definition of the interpretation has been designed so as to maintain the following important invariant.

Lemma 40. Every proposition ϕ has an interpretation

$$[\![\phi]\!] = \{R, E \in \mathsf{CStates} \mid R, E \vDash \phi\}$$

that is an upper set with respect to the order $\sqsubseteq$ on states.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

We write $R, E \overset{\mathbf{MBIi}}{\equiv} S, F$ whenever given states R, E and S, F satisfy exactly the same **MBIi**-formulae. We write $E \overset{\mathbf{MBIi}}{\equiv} F$ whenever the processes E and F satisfy the same formulae at all R.

Theorem 41. If $E \sim F$, then $E \overset{\mathbf{MBIi}}{\equiv} F$.

The proof is essentially as in the classical case, with a few easy modifications because of the new interpretation. This shows that the set $[\![\phi]\!]$ is $\sim$-closed for each ϕ. Thus, an interpretation is a function

$$[\![-]\!] : \mathsf{Prop} \longrightarrow \Upsilon_{\sim}(\mathsf{CStates})$$

given any valuation.

Lemma 30, which says that the interpretation of substitution in a context is monotonic, holds in this setting. Lemma 31 also holds, by a proof that makes use of Theorem 41. The proof of soundness is also a trivial modification of the discrete version (Theorem 32). In particular, we have retained the important systems rule $(\langle - \rangle *)$ through our set-up.

Theorem 42. The calculus **MBIi** has a sound interpretation on CStates.

Quantifiers may easily be included in the system **MBIi**: the interpretation of quantifiers in **MBIc** are modified in the obvious way so that they become upper sets of states. All of the above results then continue to hold. Just as in the discrete case, it is the extension properties that make the unit axioms for the logic work. Here, however, we also need the order-extension property to get the associativity of $\times$. Thus, in situations where it is not appropriate to use the piggybacking condition, we must have a variant calculus in which this extension property is explicitly included as a structural transition rule. Note that when the order $\sqsubseteq$ on resources is taken to be discrete, **OSCRP** reduces to **SCRPr**, and the interpretation of formulae of **MBIi** are identical to their interpretation in **MBIc**. Thus the discrete versions are special cases of the ordered versions.

Example 43. The fact that all propositions are upper sets can be very useful for model-checking, since, for example, it sometimes suffices to verify that the given state has sufficient resource. Consider, for example, a language with just increment i and decrement d operations over the resource monoid consisting of the natural numbers with their usual ordering. If we take

$$\mu(d^m i^n, p) = \begin{cases} p + n - m & \text{if } m \leqslant p \\ \uparrow & \text{if } m > p, \end{cases}$$

then μ is a modification in the sense of this section. Because of the particular properties of this resource monoid, we do not get any more transitions than we did for the unordered calculus. However, we may take typical atomic propositions from the logical language to make assertions like ϕ_n, where this says 'the resource component of the given state is greater than n'. Propositions can then be checked at states by combinations of computable order-assertions. A proposition of the form $\langle ab \rangle(\phi_m * \phi_n)$ can be checked by finding a witness for $\langle a \rangle \phi_m * \langle b \rangle \phi_n$ at a state with a sufficiently large resource component. For example, suppose we are given the state $3, (d : E) \times (i : F)$. Then we find that this state

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

satisfies $\langle d\rangle\phi_2 * \langle i\rangle\phi_1$ and $\langle di\rangle(\phi_2 * \phi_1)$. Moreover, any state $p, (d : E) \times (i : F)$ with $p \geqslant 3$ will also satisfy these properties.

5. Definable extensions

The calculus SCCS is so powerful that it can be used to capture many other frameworks for concurrent modelling and computation. Indeed, there is a remarkable functional completeness result showing that all concurrent behaviour that can be described by calculi with operational rules of a certain form are already captured by SCCS (de Simone 1985). Nevertheless, specialised calculi remain very interesting in applications, and it is an extremely pleasing aspect of (S)CCS that it may be used to give an unambiguous semantics to these calculi (Milner 1980; 1983; 1989). In this section we show how similar definability results are possible for our resource-based process calculi.

For the purposes of this section we use a synchronous calculus **SCRP**v, which is a slightly altered version of **SCRP**. A modification for **SCRP**v is therefore a partial function $\mu : \mathsf{Act} \times \mathbf{R} \longrightarrow \mathbf{R}$ satisfying the coherence conditions:

1 $\mu(1, R) = R$ for all $R \in \mathbf{R}$.
2 If $\mu(a, R)$, $\mu(b, S)$ and $R \circ S$ are defined, then $\mu(ab, R \circ S) \simeq \mu(a, R) \circ \mu(b, S)$.

The **SCRP**v hiding rule is

$$\text{Hide}\ \frac{R \circ S, E \xrightarrow{a} R' \circ S', E'}{R, vS.E \xrightarrow{vS.a} R', vS'.E'}\ (\mu(vS.a, R) = R' \downarrow)$$

Note that the hiding rule and the coherence conditions on modifications are more general than for **SCRPr**.

In Section 5.2, however, we will also employ a refinement of **SCRP**v called **SCRPr**v, which extends **SCRPr** with the Hide-id rule of **SCRP**v. This calculus is required in order to develop the theory of equivalence of asynchronous processes. In the remaining sections we will revert to **SCRP**v because the programming languages considered there do not appear to translate naturally into a system with the stronger constraint on modifications, such as **SCRPr**v.

The first additional requirement we make for **SCRP**v is that the hiding function on actions satisfies

$$vS.1 = 1$$

for all resources S. We call this the *identity-hiding* property. The example defined in equation (3) above has this property.

This calculus, **SCRP**v, has the same grammar as **SCRP**, but has one additional rule

$$\text{Hide-id}\quad \frac{}{R, vS.E \xrightarrow{1} R, vS.E}$$

added to the operational semantics of **SCRP**. Thus any hiding process may always tick given any resource. In particular, this is the case for $R, vS.E$ even when $R \circ S$ is undefined. Of course, if E was a process that could tick and composition is total, then there is no new transition of $vS.E$ given by the rule Hide-id.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

The Hide-id rule is essential for the encoding of asynchrony below. The inclusion of this rule can be compared with the restriction operator of SCCS, where in any restriction $E \upharpoonright A$ the set A must contain the tick action 1.

We use the name **SCRPr**v to refer to **SCRP**v-calculi with:

— a modification function μ that satisfies the same coherence conditions as **SCRPr** (rather than just the weaker conditions for **SCRP**);
— the side condition on hiding regarding piggybacking;
— the identity-hiding property;
— the Hide-id rule.

The following table summarises the differences between the **SCRP**-calculi used in this paper.

	coherence	piggybacking	Hide-id and identity hiding
SCRP	$\simeq$	no	no
SCRPr	$=$	yes	no
SCRPv	$\simeq$	no	yes
SCRPrv	$=$	yes	yes

It is straightforward to show that Lemma 1, Propositions 4 and 7 and Lemmas 8 and 9 hold in **SCRPr**v. The proofs are by minor modifications of those for **SCRPr**.

5.1. *Idleness and delay*

The key to the fact that the synchronous formalism of processes encodes the asynchronous formalism is the definability of processes that may tick (perform the identity action) for arbitrary finite time before performing any other action.

We begin by defining the extremely important *delay operator*, δ, which takes a process and produces another process that may wait arbitrarily long before making any non-identity action. For any E, we take

$$\delta(E) = fix\, X.((1 : X) + E)$$

to be the delayed process. Note that it may still perform an E action immediately and that if E is an agent, then so is $\delta(E)$. The delay operator satisfies two derived rules

$$\frac{}{R, \delta(E) \xrightarrow{1} R, \delta(E)} \qquad \frac{R, E \xrightarrow{a} \mu(a, R), E'}{R, \delta(E) \xrightarrow{a} \mu(a, R), E'}$$

for all actions a, resources R and processes E.

Proposition 44. The delay operator satisfies the following equalities and inequalities:

$$\delta(E) \sim \delta(\delta(E)) \sim E + 1 : \delta(E) \sim E + \delta(E)$$

$$\delta(E) \times \delta(F) \sim \delta((E \times \delta(F)) + (\delta(E) \times F))$$

$$\delta(\nu S.E) \lesssim \nu S.\delta(E)$$

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

for all processes E, F and resources S. If the partial function $R \circ - : \mathbf{R} \longrightarrow \mathbf{R}$ is injective for every $R \in \mathbf{R}$, then

$$vS.\delta(E) \sim \delta(vS.E)$$

holds for all resources S and processes E.

We omit the proof (which uses the standard techniques) but note that the property $vS.1 = 1$ is required for the relations involving hiding processes.

A state R, E is said to be *idle* if $R, E \approx R, \delta(E)$. A process E is said to be idle if R, E is idle for every resource R.

Proposition 45. For any process E:

1 A state R, E is idle if and only if $R, E \xrightarrow{1} R, E$.
2 A process E is idle if and only if $E \approx \delta(E)$.
3 A process E is idle if and only if $E \sim \delta(E)$.

Proof.

1 This is immediate by the definition of δ.
2 This is immediate by the definition of $\approx$ on processes.
3 If $E \sim \delta(E)$, then $E \approx \delta(E)$ since Lemma 8 holds here, so we may apply (2) and conclude that E is idle. Now suppose that E is idle. If $R, E \xrightarrow{a} R, F$, then $R, \delta(E) \xrightarrow{a} R, F$ and $F \sim F$. If $R, \delta(E) \xrightarrow{a} R, F$, then either $R, E \xrightarrow{a} R, F$ or $a = 1$ and $F = \delta(E)$. In the first case there is nothing to show, and in the second we have $R, E \xrightarrow{1} R, E$. Hence $E \sim \delta(E)$. □

Lemma 46. For all processes E and F:

1 $\delta(E)$ is idle.
2 $vS.E$ is idle.
3 If E and F are idle, then $E \times F$ is idle.

Proof. All three parts follow from Lemma 45:

1 This is immediate by reflexivity of $\approx$.
2 This is immediate by the Hide-id rule.
3 This follows by the operational rule for product processes since any resource R decomposes into a pair (R, e) with $R \circ e = R$. □

Recall that in Milner (1983) a process is said to be asynchronous if every proper derivative is idle. We make an appropriate change to this for all **SCRP** calculi. We define a state to be *asynchronous* if every proper derivative of that state is idle. A process E is *asynchronous* when all E-states are asynchronous.

5.2. *Asynchronous prefix*

For the purposes of this section we assume that the action monoid Act contains countably many tick actions (actions b such that $\mu(b, R) = R$ for all resources R). This is mostly harmless in the light of the following proposition.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

Proposition 47. Let **R** be a resource monoid, Act an action monoid, μ be a modification (of **SCRP**v) and v be a hiding function. Let B be any set disjoint from Act. The action set may be freely extended with B giving a new action monoid Act′, a new modification $\mu' : \mathsf{Act}' \times \mathbf{R} \longrightarrow \mathbf{R}$ and a new hiding $v' : \mathbf{R} \times \mathsf{Act}' \longrightarrow \mathsf{Act}'$ such that:

— μ' and v' agree with μ and v, respectively on Act.
— B contains only tick actions.

Furthermore, if μ is a **SCRPr**v modification, then so is μ'.

Proof. Let Act′ be the free monoid of words over the set $\mathsf{Act} \cup B$. Words are written in the form $\langle x_1, \ldots, x_n \rangle$, the unit word is $\langle\rangle$ and multiplication is concatenation of words. For any word w, let $\divideontimes w = \prod(x_i \mid w \equiv \langle x_1, \ldots, x_n \rangle \ \& \ 1 \leqslant i \leqslant n \ \& \ x_i \notin B)$ be the action of Act formed by forgetting all letters from B and replacing formal products by products of Act. In particular, $\divideontimes\langle\rangle = 1$, the unit of Act. We define

$$\begin{aligned} \mu'(w, R) &\simeq \mu(\divideontimes w, R) \\ v'S.w &\simeq vS.(\divideontimes w) \end{aligned}$$

for all words w and resources R and S.

For any S, we have $v'S.\langle\rangle = vS.1 = 1$, so v' is a hiding (it satisfies the identity-hiding property).

Note that $\mu'(\langle\rangle, R) = \mu(1, R) = R$ for all R.

Suppose that $\mu'(v, R)$, $\mu'(w, S)$ and $R \circ S$ are all defined. Since μ is a modification, $\mu((\divideontimes v)(\divideontimes w), R \circ S)) \simeq \mu(\divideontimes v, R) \circ \mu(\divideontimes w, S)$. Now $\divideontimes(vw) = (\divideontimes v)(\divideontimes w)$, so

$$\begin{aligned} \mu'(vw, R \circ S) &\simeq \mu(\divideontimes(vw), R \circ S) \\ &\simeq \mu((\divideontimes v)(\divideontimes w), R \circ S) \\ &\simeq \mu(\divideontimes v, R) \circ \mu(\divideontimes w, S) \\ &\simeq \mu'(v, R) \circ \mu'(w, S) \end{aligned}$$

and μ' is a modification.

If μ is a **SCRPr**v modification, then each instance of $\simeq$ above can be replaced by an equality since both sides of each equality are defined, and so μ' is a **SCRPr**v modification.

Finally, $\mu'(\langle b \rangle, R) = \mu(1, R) = R$, for every $b \in B$ and $R \in \mathbf{R}$. □

We now define the asynchronous calculus **ASCRP**. This calculus is the analogue for **SCRP**v of the calculus ASCCS presented in Milner (1983).

The grammar of the new language is

$$E ::= X \mid a.E \mid \delta(E) \mid \sum_{i \in I} E_i \mid E \times E \mid vR.E \mid fix_i \mathsf{X}.\mathsf{E}$$

where the notation for variables and processes is as before, and this calculus is to be considered relative to a fixed $(\mathsf{Act}, \mathbf{R}, \mu, v)$. The operator δ could have been omitted since it is definable. We take 0 to be the sum of an empty set of processes and 1 to be $\delta(0)$. This will turn out to be equivalent to $fix\, X.(1.X)$.

We give a semantics to this calculus by translating into **SCRP**v over the same signature $(\mathsf{Act}, \mathbf{R}, \mu, v)$. We define this translation $\mathscr{T}_{as} : \mathbf{ASCRP} \longrightarrow \mathbf{SCRP}v$ recursively by the clause

$$\mathscr{T}_{as}(a.E) \ = \ a : \delta(\mathscr{T}_{as}(E)),$$

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

together with clauses such that $\mathscr{T}_{as}$ passes through all the other process combinators:

$$\begin{aligned}
\mathscr{T}_{as}(X) &= X \\
\mathscr{T}_{as}(\delta(E)) &= \delta(\mathscr{T}_{as}(E)) \\
\mathscr{T}_{as}\left(\sum E_i\right) &= \sum \mathscr{T}_{as}(E_i) \\
\mathscr{T}_{as}(E \times F) &= \mathscr{T}_{as}(E) \times \mathscr{T}_{as}(F) \\
\mathscr{T}_{as}(\nu R.E) &= \nu R.\mathscr{T}_{as}(E) \\
\mathscr{T}_{as}(fix_i \mathsf{X}.\mathsf{E}) &= fix_i \mathsf{X}.\mathscr{T}_{as}(\mathsf{E}),
\end{aligned}$$

where the final equality uses the evident tuple of translations of each of the components.

The semantics of **ASCRP** is defined by the operational rules inherited from **SCRP**v. To be precise, the transitions of an **ASCRP** state R, E are induced from **SCRP**v-transitions of the form

$$R, \mathscr{T}_{as}(E) \xrightarrow{a} R', E'$$

where R', E' is a **SCRP**v-state. We then have the following proposition to show that the calculus **ASCRP** contains only asynchronous processes and is suitably closed under transitions.

Proposition 48. If E is an agent of **ASCRP** and $R, \mathscr{T}_{as}(E) \xrightarrow{a} R', E'$ for some R, R', then E' is the translation of an agent of **ASCRP** and E' is idle. In particular, R', E' is idle.

Proof. The proof is by induction on the structure of the agent E of **ASCRP**. The prefixing case itself is a simple consequence of the properties of δ. The Hide-id rule ensures that the derivative of any hiding is idle. The other details are all routine. □

As an example of the above translations at work, observe that an **ASCRP**-state of the form $R, a.b.1$ gives a sequence of **SCRP**v-transitions

$$R, a : \delta(b : \delta(1)) \xrightarrow{a} \mu(a, R), \delta(b : \delta(1)) \xrightarrow{b} \mu(b, \mu(a, R)), \delta(1)$$

when $\mu(b, \mu(a, R))$ is defined, making use of the Prefix rule and one of the derived rules for δ.

It is often inappropriate to use either of the relations $\sim$ and $\approx$ to compare agents in such definable asynchronous calculi since agents that delay by differing times should not necessarily be distinguished. In particular, the unit action 1 should be invisible from the point of view of the equivalence.

The remainder of the work in this subsection is concerned with the study of equivalence relations for asynchronous processes. For this we suppose that the translation is, in fact, into a member of **SCRPr**v. In particular, the modification satisfies the stronger version of coherence. The reason for this is that we wish to find an equivalence that is a congruence, so we want the property that if two asynchronous processes are equivalent, then they cannot be distinguished by forming the product with any other asynchronous process. A step in our construction is to find a bisimulation relation that identifies any asynchronous process E with $E \times 1$, and this requires the simple-extension property for transitions. An alternative might be to work with a calculus in which the simple-extension property is

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

taken as one of the rules defining the operational semantics, but this avenue has not been explored.

For any set X, let X^* be the set of all finite words on X. Let $u \in \mathsf{Act}^*$ be the word $\langle a_1, \ldots, a_i, a_{i+1}, \ldots, a_n \rangle$. For any **SCRPr**$v$-states R, E and R', E', we write

$$R, E \stackrel{u}{\Longrightarrow} R', E'$$

just when there is some sequence of transitions

$$R, E(\stackrel{1}{\rightarrow})^* \stackrel{a_1}{\rightarrow} (\stackrel{1}{\rightarrow})^* \ldots (\stackrel{1}{\rightarrow})^* \stackrel{a_n}{\rightarrow} (\stackrel{1}{\rightarrow})^* R', E',$$

or, in other words, if there is a sequence of transitions along a_1 to a_n in order, but interspersed with arbitrarily many tick actions. In particular, $R, E \stackrel{\langle\rangle}{\Longrightarrow} R, E$ where $\langle\rangle$ is the empty word. We write $R, E \stackrel{a}{\Longrightarrow} R', E'$ when $R, E \stackrel{u}{\Longrightarrow} R', E'$ with $u = \langle a \rangle$. We write $R, E \stackrel{a}{\rightarrow}\stackrel{u}{\Longrightarrow} R', E'$ for a sequence of transitions that begins with an a-transition and ends with a sequence of transitions from u (interspersed by ticks).

We define the relation $\sim_{\mathrm{a}}$ to be the largest binary relation on **SCRPr**v agents such that whenever $R, R' \in \mathbf{R}$, $u \in (\mathsf{Act} \setminus \{1\})^*$ and $E \sim_{\mathrm{a}} F$:

— if there is some E' with $R, E \stackrel{u}{\Longrightarrow} R', E'$, then there is some F' with $R, F \stackrel{u}{\Longrightarrow} R', F'$ and $E' \sim_{\mathrm{a}} F'$;
— if there is some F' with $R, F \stackrel{u}{\Longrightarrow} R', F'$, then there is some E' with $R, E \stackrel{u}{\Longrightarrow} R', E'$ and $E' \sim_{\mathrm{a}} F'$.

The relation is then extended to all processes in the standard way (by substitution). Any relation contained in $\sim_{\mathrm{a}}$ is said to be a *weak global bisimulation* or WG-bisimulation, for short.

This relation is an equivalence. Furthermore, any pair of processes that differ only by a number of ticks inserted as prefixes will be equivalent under this relation. However, such pairs of processes can be distinguished by the use of the synchronous parallel composition $\times$. The sequence of results that follow study a congruence formed from $\sim_{\mathrm{a}}$ by closing under substitution in all asynchronous contexts. These results are analogues for **ASCRP** of those in the theory of ASCCS in Milner (1983, Section 8, pages 296–301). The proof of the first proposition below is just an unwinding of the definition of WG-bisimulation; the second, third and fourth propositions are implied by the first.

Proposition 49. A relation $\sim'$ is contained in $\sim_{\mathrm{a}}$ if and only if whenever $R \in \mathbf{R}$ and $E \sim' F$, then:

— If $R, E \stackrel{a}{\rightarrow} \mu(a, R), E'$ for some E', then either $a = 1$ and $E' \sim' F$ or there is some F' with $R, F \stackrel{a}{\Longrightarrow} \mu(a, R), F'$ and $E' \sim' F'$.
— If $R, F \stackrel{a}{\rightarrow} \mu(a, R), F'$ for some F', then either $a = 1$ and $E \sim' F'$ or there is some E' with $R, E \stackrel{a}{\Longrightarrow} \mu(a, R), E'$ and $E' \sim' F'$.

Proposition 50. The relation $\sim$ is contained in $\sim_a$.

Proposition 51. Let E be an agent of **ASCRP**. Then

$$\mathscr{T}_{as}(E) \sim_{\mathrm{a}} 1 : \mathscr{T}_{as}(E) \sim_{\mathrm{a}} \mathscr{T}_{as}(1.E) \sim_{\mathrm{a}} \delta(\mathscr{T}_{as}(E)).$$

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

Proposition 52. If $\mathscr{T}_{as}(E) \sim_{\mathrm{a}} \mathscr{T}_{as}F$, then

$$\mathscr{T}_{as}(a.E) \sim_{\mathrm{a}} \mathscr{T}_{as}(a.F) \qquad \mathscr{T}_{as}(\delta(E)) \sim_{\mathrm{a}} \mathscr{T}_{as}(\delta(F)) \qquad \mathscr{T}_{as}(\nu S.E) \sim_{\mathrm{a}} \mathscr{T}_{as}(\nu S.F)$$

all hold.

The simple-extension property of Proposition 4 together with Proposition 49 gives the following result (which also follows from Proposition 50).

Lemma 53. The relation $E \sim_{\mathrm{a}} E \times 1$ holds for all **SCRPr**ν-processes E.

Lemma 54. Suppose that E, F and G are idle processes of **SCRPr**ν. If $E \sim_{\mathrm{a}} F$, then $E \times G \sim_{\mathrm{a}} F \times G$.

Proof. The characterisation of Proposition 49 is used for the relation $\sim'$, which is defined for all E, F and G, by

$$E \times G \sim' F \times G \iff E \sim_{\mathrm{a}} F \text{ and } E, F, G \text{ are idle},$$

and only for such processes. If some transition $R, E \times G \xrightarrow{a} \mu(a, R), E' \times G'$ takes place, then this splits into a transition for E and a transition for G using the operational rule for products. Since $E \sim_{\mathrm{a}} F$, one can apply Proposition 49 to find a sequence of transitions from F into some F' with $E' \sim_{\mathrm{a}} F'$, otherwise we have that $E' \sim_{\mathrm{a}} F$ and the E-state ticks, with $a = 1$. In the first case, the fact that G is idle gives a sequence of matching length from G and hence $R, F \times G \stackrel{a}{\Longrightarrow} \mu(a, R), F' \times G'$ with $E' \times G' \sim' F' \times G'$. In the second case, we get $R, F \times G \xrightarrow{a} \mu(a, R), F \times G'$ and $E' \times G' \sim' F \times G$ since E', F, G' are idle. The verification of the other condition (when $R, F \times G$ make some transition) is similar. □

Lemma 55. The following statements are equivalent:

1 For all agents G of **ASCRP**, the relation $\mathscr{T}_{as}(E \times G) \sim_{\mathrm{a}} \mathscr{T}_{as}(F \times G)$ holds.
2 For all $a \in \mathsf{Act}$ and all $R \in \mathbf{R}$:
   — if $R, \mathscr{T}_{as}(E) \xrightarrow{a} \mu(a, R), E'$ for some E', then $R, \mathscr{T}_{as}(F) \xrightarrow{a} \stackrel{\langle\rangle}{\Longrightarrow} \mu(a, R), F'$ for some F' with $E' \sim_{\mathrm{a}} F'$;
   — if $R, \mathscr{T}_{as}(F) \xrightarrow{a} \mu(a, R), F'$ for some F', then $R, \mathscr{T}_{as}(E) \xrightarrow{a} \stackrel{\langle\rangle}{\Longrightarrow} \mu(a, R), E'$ for some E' with $E' \sim_{\mathrm{a}} F'$.

Proof. Suppose (2) is true and that there is some transition of an $\mathscr{T}_{as}(E \times G)$-state. Such a transition must be of the form

$$\frac{R, \mathscr{T}_{as}(E) \xrightarrow{a} \mu(a, R), E' \qquad S, \mathscr{T}_{as}(G) \xrightarrow{b} \mu(b, S), G'}{R \circ S, \mathscr{T}_{as}(E \times G) \xrightarrow{ab} \mu(ab, R \circ S), E' \times G'}$$

for some a, b, R, S, E', G'. By (2), there is some F' with $R, \mathscr{T}_{as}(F) \xrightarrow{a} \stackrel{\langle\rangle}{\Longrightarrow} \mu(a, R), F'$ for some F' with $E' \sim_{\mathrm{a}} F'$. So $R, \mathscr{T}_{as}(F) \xrightarrow{a} \stackrel{1}{(\rightarrow)}{}^{n} \mu(a, R), F'$ for some n. Now G' is idle by Proposition 48, so $S, \mathscr{T}_{as}(G) \xrightarrow{b} \stackrel{1}{(\rightarrow)}{}^{n} \mu(b, S), G'$. Therefore

$$R \circ S, \mathscr{T}_{as}(F \times G) \xrightarrow{ab} \stackrel{\langle\rangle}{\Longrightarrow} \mu(ab, R \circ S), F' \times G'$$

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

and

$$E' \times G' \sim_{\mathrm{a}} F' \times G'$$

by Lemma 54, since E' and F' are idle by Proposition 48. A similar argument can be made when given any transition of any $\mathscr{T}_{as}(F \times G)$-state, so (1) holds by Proposition 49.

Now suppose that (2) is false. Without loss of generality, we can suppose that it is the first of the two conditions that fails. Since we have infinitely many tick actions, there must be some such tick b not present in F. Take $G = b.\mathsf{0}$. Then $R, \mathscr{T}_{as}(E \times G) \xrightarrow{ab} \mu(ab, R), E' \times \mathsf{1}$ for some E'. If $R, \mathscr{T}_{as}(F \times G) \stackrel{\langle ab \rangle}{\Longrightarrow} \mu(ab, R), F' \times \mathsf{1}$ for some F', we must have $R, \mathscr{T}_{as}(F) \xrightarrow{a} \stackrel{\langle\rangle}{\Longrightarrow} \mu(a, R), F'$. Since (2) is false, we have $E' \not\sim_{\mathrm{a}} F'$. Then $E' \times \mathsf{1} \not\sim_{\mathrm{a}} F' \times \mathsf{1}$ by Lemma 53. Therefore $\mathscr{T}_{as}(E \times G) \not\sim_{\mathrm{a}} \mathscr{T}_{as}(F \times G)$, and (1) does not hold. □

Let E, F be processes of **ASCRP**. We define $E \sim_{\mathrm{a}}^{\times} F$ if for every agent G of **ASCRP** the relation $\mathscr{T}_{as}(E \times G) \sim_{\mathrm{a}} \mathscr{T}_{as}(F \times G)$ holds. The first lemma below is immediate, and the second holds by taking $G = \mathsf{1}$ and applying Lemma 53.

Lemma 56. Let X contain precisely the free variables of E and F. Then $E \sim_{\mathrm{a}}^{\times} F$ if and only if $E[\mathsf{H}/\mathsf{X}] \sim_{\mathrm{a}}^{\times} F[\mathsf{H}/\mathsf{X}]$ for all tuples of **ASCRP** agents with length matching X.

Lemma 57. If $E \sim_{\mathrm{a}}^{\times} F$, then $\mathscr{T}_{as}(E) \sim_{\mathrm{a}} \mathscr{T}_{as}(F)$.

Lemma 58. The relation $\sim_{\mathrm{a}}^{\times}$ is a congruence on **ASCRP**-processes:

1 If $E \sim_{\mathrm{a}}^{\times} F$, then the following hold:
   (a) $a.E \sim_{\mathrm{a}}^{\times} a.F$
   (b) $\delta(E) \sim_{\mathrm{a}}^{\times} \delta(F)$
   (c) $E \times G \sim_{\mathrm{a}}^{\times} F \times G$
   (d) $vS.E \sim_{\mathrm{a}}^{\times} vS.F$.
2 If $E_i \sim_{\mathrm{a}}^{\times} F_i$ for all $i \in I$, then $\sum_{i \in I} E_i \sim_{\mathrm{a}}^{\times} \sum_{i \in I} F_i$ holds.
3 If $\mathsf{E} \sim_{\mathrm{a}}^{\times} \mathsf{F}$, then $fix_i \mathsf{X}.\mathsf{E} \sim_{\mathrm{a}}^{\times} fix_i \mathsf{X}.\mathsf{F}$ holds.

Proof. Suppose $E \sim_{\mathrm{a}}^{\times} F$.

A simple proof that $a.E \sim_{\mathrm{a}}^{\times} a.F$ uses the characterisation of Lemma 55 and the fact that $\mathscr{T}_{as}(\delta(E)) \sim_{\mathrm{a}} \mathscr{T}_{as}(\delta(F))$ by Proposition 52.

In order to show that $\delta(E) \sim_{\mathrm{a}}^{\times} \delta(F)$, we show that

$$\delta(\mathscr{T}_{as}(E)) \times \mathscr{T}_{as}(H) \sim_{\mathrm{a}} \delta(\mathscr{T}_{as}(F)) \times \mathscr{T}_{as}(H)$$

for an arbitrary agent H of **ASCRP**. Supposing we have a transition of $\delta(\mathscr{T}_{as}(E)) \times \mathscr{T}_{as}(H) \xrightarrow{ab} \mu(ab, R), K$, there must be a decomposition as an a-transition of a $\delta(\mathscr{T}_{as}(E))$-state and b-transition of a $\mathscr{T}_{as}(H)$-state. Now $\mathscr{T}_{as}(\delta(E)) \sim_{\mathrm{a}} \mathscr{T}_{as}(\delta(F))$ by Proposition 52, so the characterisation of Proposition 49 may then be applied. In either case of Proposition 49, we get $\delta(\mathscr{T}_{as}(F)) \times \mathscr{T}_{as}(H) \xrightarrow{ab} \Longrightarrow \mu(ab, R), K$ (using Lemma 54 in the idle case $a = 1$). The symmetrical argument for when $\delta(\mathscr{T}_{as}(F)) \times \mathscr{T}_{as}(H)$ makes a transition, and an application of Proposition 49 once more gives the desired conclusion.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

Now

$$\mathscr{T}_{as}((E \times G) \times H) \sim_{\mathrm{a}} \mathscr{T}_{as}((F \times G) \times H)$$

for an arbitrary agent H of **ASCRP** follows from

$$(\mathscr{T}_{as}(E) \times \mathscr{T}_{as}(G)) \times \mathscr{T}_{as}(H) \sim_{\mathrm{a}} \mathscr{T}_{as}(E) \times (\mathscr{T}_{as}(G) \times \mathscr{T}_{as}(H))$$

and

$$\mathscr{T}_{as}(F) \times (\mathscr{T}_{as}(G) \times \mathscr{T}_{as}(H)) \sim_{\mathrm{a}} (\mathscr{T}_{as}(F) \times \mathscr{T}_{as}(G)) \times \mathscr{T}_{as}(H)$$

since $\sim$ is contained in $\sim_{\mathrm{a}}$, and the definition of $\sim_{\mathrm{a}}^{\times}$.

Proposition 52 gives $\nu S.\mathscr{T}_{as}(E) \sim_{\mathrm{a}} \nu S.\mathscr{T}_{as}(F)$. Propositions 48 and 49 and Lemma 54 can then be used to show that

$$\nu S.\mathscr{T}_{as}(E) \times \mathscr{T}_{as}(H) \sim_{\mathrm{a}} \nu S.\mathscr{T}_{as}(F) \times \mathscr{T}_{as}(H)$$

for any agent H of **ASCRP**. Hence $\nu S.E \sim_{\mathrm{a}}^{\times} \nu S.F$.

Suppose now that $E_i \sim_{\mathrm{a}}^{\times} F_i$ for all $i \in I$. To show $\sum_{i\in I} E_i \sim_{\mathrm{a}}^{\times} \sum_{i\in I} F_i$ holds, it suffices to show that

$$\mathscr{T}_{as}\left(\sum_{i\in I} E_i\right) \times \mathscr{T}_{as}(H) \sim_{\mathrm{a}}^{\times} \mathscr{T}_{as}\left(\sum_{i\in I} F_i\right) \times \mathscr{T}_{as}(H)$$

holds for any agent H of **ASCRP**. But now any transition of the component

$$R, \mathscr{T}_{as}\left(\sum_{i\in I} E_i\right) \xrightarrow{a} \mu(a, R), E'$$

with some given resource R comes from some

$$R, \mathscr{T}_{as}(E_i) \xrightarrow{a} \mu(a, R), E'.$$

By Lemma 55, this is matched by

$$R, \mathscr{T}_{as}(F_i) \xrightarrow{a}\!\!\Longrightarrow \mu(a, R), F'$$

for some $F' \sim_{\mathrm{a}} E'$. But then

$$R, \mathscr{T}_{as}\left(\sum_{i\in I} F_i\right) \xrightarrow{a} \mu(a, R), F',$$

and thus

$$\mathscr{T}_{as}\left(\sum_{i\in I} E_i\right) \times \mathscr{T}_{as}(H) \sim_{\mathrm{a}}^{\times} \mathscr{T}_{as}\left(\sum_{i\in I} F_i\right) \times \mathscr{T}_{as}(H)$$

by Lemma 55.

Now suppose that $\mathsf{E} \sim_{\mathrm{a}}^{\times} \mathsf{F}$. Consider the relation $\sim'$ on **SCRPr**v processes defined by pairs of the form

$$\mathscr{T}_{as}(G[\mathit{fix}\,\mathsf{X}.\mathsf{E}/\mathsf{Y}]) \sim' \mathscr{T}_{as}(G[\mathit{fix}\,\mathsf{X}.\mathsf{F}/\mathsf{Y}])$$

such that G is any **ASCRP** term with all free variables in Y. We define a further relation $\sim_{\mathrm{a}}'$ by

$$E \sim_{\mathrm{a}}' H \quad \Longleftrightarrow \quad \exists F, G.\ \ E \sim_{\mathrm{a}} F \sim' G \sim_{\mathrm{a}} H$$

for all **SCRPr**v-processes E, F, G, H.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

Below we show by induction that the property

$$\begin{array}{l}\text{if } R, \mathscr{T}_{as}(G[fix\,\mathsf{X}.\mathsf{E}/\mathsf{Y}]) \xrightarrow{a} \mu(a,R), E', \text{ then for some idle } F' \text{ and } G' \text{ we have} \\ R, \mathscr{T}_{as}(G[fix\,\mathsf{X}.\mathsf{F}/\mathsf{Y}]) \xrightarrow{a}\!\!\Longrightarrow \mu(a,R), G' \text{ and } E' \sim' F' \sim_{\mathrm{a}} G'\end{array} \tag{7}$$

holds.

It follows from property (7) that $\sim'_{\mathrm{a}}$ is a WG-bisimulation, that is, $\sim'_{\mathrm{a}} \subseteq \sim_{\mathrm{a}}$. Taking $G = Y_i$ then gives the special case

$$\begin{array}{l}\text{if } R, \mathscr{T}_{as}(fix_i\mathsf{X}.\mathsf{E}) \xrightarrow{a} \mu(a,R), E', \text{ then for some idle } F' \text{ we have} \\ R, \mathscr{T}_{as}(fix_i\mathsf{X}.\mathsf{F}) \xrightarrow{a}\!\!\Longrightarrow \mu(a,R), F' \text{ and } E' \sim_a F'.\end{array}$$

The symmetric property to this and the characterisation of Lemma 55 then shows that $fix_i\mathsf{X}.\mathsf{E} \sim^{\times}_{\mathrm{a}} fix_i\mathsf{X}.\mathsf{F}$, as required.

We now prove property (7) by induction on the inference of $R, \mathscr{T}_{as}(G[fix_i\mathsf{X}.\mathsf{E}/\mathsf{Y}]) \xrightarrow{a} \mu(a,R), E'$:

$G = Y_i$

We have $R, \mathscr{T}_{as}(fix_i\mathsf{X}.\mathsf{E}) \xrightarrow{a} \mu(a,R), E'$, so $R, \mathscr{T}_{as}(E_i)[fix\,\mathsf{X}.\mathscr{T}_{as}(\mathsf{E})/\mathsf{X}] \xrightarrow{a} \mu(a,R), E'$ by a shorter inference. Then $R, \mathscr{T}_{as}(F_i)[fix\,\mathsf{X}.\mathscr{T}_{as}(\mathsf{F})/\mathsf{X}] \xrightarrow{a}\!\!\Longrightarrow \mu(a,R), F'$ with $E' \sim' H' \sim_{\mathrm{a}} F'$ for some idle H', F', by the induction hypothesis. Therefore there is a transition $R, \mathscr{T}_{as}(fix_i\mathsf{X}.\mathsf{F}) \xrightarrow{a} \mu(a,R), F'$.

$G = \delta(G_0)$

We omit this case since δ is definable.

$G = a.G_0$

We have $R, \mathscr{T}_{as}(G_0[fix\,\mathsf{X}.\mathsf{E}/\mathsf{Y}]) \xrightarrow{a} \mu(a,R), E'$. This is the same as

$$R, a : \delta(\mathscr{T}_{as}(G_0[fix\,\mathsf{X}.\mathsf{E}/\mathsf{Y}])) \xrightarrow{a} \mu(a,R), \delta(\mathscr{T}_{as}(G_0[fix\,\mathsf{X}.\mathsf{E}/\mathsf{Y}]))$$

with $\mu(a,R)$ defined. Then

$$R, a : \delta(\mathscr{T}_{as}(G_0[fix\,\mathsf{X}.\mathsf{F}/\mathsf{Y}])) \xrightarrow{a} \mu(a,R), \delta(\mathscr{T}_{as}(G_0[fix\,\mathsf{X}.\mathsf{F}/\mathsf{Y}]))$$

and

$$\begin{array}{rcl}\delta(\mathscr{T}_{as}(G_0[fix\,\mathsf{X}.\mathsf{E}/\mathsf{Y}])) & = & \mathscr{T}_{as}(\delta(G_0[fix\,\mathsf{X}.\mathsf{E}/\mathsf{Y}])) \\ & \sim' & \mathscr{T}_{as}(\delta(G_0[fix\,\mathsf{X}.\mathsf{F}/\mathsf{Y}])) \\ & = & \delta(\mathscr{T}_{as}(G_0[fix\,\mathsf{X}.\mathsf{F}/\mathsf{Y}])),\end{array}$$

as required.

$G = G_0 \times G_1$

The product case uses the Product rule to split product transitions into pairs of transitions, the induction hypothesis on those pairs, the easy fact that $\sim'$ is preserved by products and the fact that $\sim^{\times}_{\mathrm{a}}$ is a congruence for $\times$ (part 1(c) of this Lemma).

$G = \sum_{i\in I} G_i$

This case follows by a straightforward application of the induction hypothesis.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

$G = \nu S.G_0$

Suppose $R, \mathscr{T}_{as}(\nu S.G_0[fix\,\mathsf{X}.\mathsf{E}/\mathsf{Y}]) \xrightarrow{a} \mu(a, R), E'$. This is the same as

$$R, \nu S.\mathscr{T}_{as}(G_0[fix\,\mathsf{X}.\mathsf{E}/\mathsf{Y}]) \xrightarrow{a} \mu(a, R), E'.$$

There are two rules from which we may derive such a transition. If we use the Hide-id rule with $a = 1$ and $E' = \nu S.\mathscr{T}_{as}(G_0[fix\,\mathsf{X}.\mathsf{E}/\mathsf{Y}])$, then, evidently,

$$R, \nu S.\mathscr{T}_{as}(G_0[fix\,\mathsf{X}.\mathsf{F}/\mathsf{Y}]) \xrightarrow{1} \mu(a, R), F'$$

and $E' \sim' F' \sim_{\mathrm{a}} F'$ with

$$F' = \nu S.\mathscr{T}_{as}(G_0[fix\,\mathsf{X}.\mathsf{F}/\mathsf{Y}]).$$

On the other hand, if the Hide rule was used to derive the given transition, there must be some b, S', E'_0 such that

$$R \circ S, \mathscr{T}_{as}(G_0[fix\,\mathsf{X}.\mathsf{E}/\mathsf{Y}]) \xrightarrow{b} \mu(a, R) \circ S', E'_0,$$

where $a = \nu S.b$, $E' = \nu S'.E'_0$ and the side conditions for the rule hold. By the induction hypothesis we have

$$R \circ S, \mathscr{T}_{as}(G_0[fix\,\mathsf{X}.\mathsf{F}/\mathsf{Y}]) \xrightarrow{b} \mu(a, R) \circ S', F'_0$$

for some F'_0, G'_0 with $E'_0 \sim' F'_0 \sim_{\mathrm{a}} G'_0$. Then

$$R, \nu S.\mathscr{T}_{as}(G_0[fix\,\mathsf{X}.\mathsf{F}/\mathsf{Y}]) \xrightarrow{a}\!\!\Longrightarrow \mu(a, R), \nu S'.F'_0$$

by the Hide rule (since the side conditions are exactly the same as the previous side conditions). So

$$R, \mathscr{T}_{as}(\nu S.G_0[fix\,\mathsf{X}.\mathsf{F}/\mathsf{Y}]) \xrightarrow{a}\!\!\Longrightarrow \mu(a, R), F'$$

with $F' = \nu S'.F'_0$. The fact that $E' \sim' F'$ follows easily from $E'_0 \sim' F'_0$, and then $F' \sim_{\mathrm{a}} G'$ follows since $\sim_{\mathrm{a}}$ is a congruence for ν (part 1(d) of this Lemma).

$G = fix_j\mathsf{Z}.\mathsf{H}$, where X, Y and Z have no variables in common.

Suppose there is a transition

$$R, \mathscr{T}_{as}((fix_j\mathsf{Z}.\mathsf{H})[fix\,\mathsf{X}.\mathsf{E}/\mathsf{Y}]) \xrightarrow{a} \mu(a, R), E'.$$

This is identical to

$$R, fix_j\mathsf{Z}.\mathscr{T}_{as}(\mathsf{H}[fix\,\mathsf{X}.\mathsf{E}/\mathsf{Y}]) \xrightarrow{a} \mu(a, R), E'.$$

Then there is a shorter inference with

$$R, (\mathscr{T}_{as}(H_j[fix\,\mathsf{X}.\mathsf{E}/\mathsf{Y}]))[(fix\,\mathsf{Z}.\mathscr{T}_{as}(\mathsf{H}[fix\,\mathsf{X}.\mathsf{E}/\mathsf{Y}]))/\mathsf{Z}] \xrightarrow{a} \mu(a, R), E'.$$

Letting $\mathsf{G} = fix\mathsf{Z}.\mathsf{H}$, this is

$$R, \mathscr{T}_{as}(H_j[\mathsf{G}/\mathsf{Z}][fix_i\mathsf{X}.\mathsf{E}/Y]) \xrightarrow{a} \mu(a, R), E'.$$

Then

$$R, \mathscr{T}_{as}(H_j[\mathsf{G}/\mathsf{Z}][fix_i\mathsf{X}.\mathsf{F}/Y]) \xrightarrow{a} \mu(a, R), G'$$

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

with $E' \sim' F' \sim_{\mathrm{a}} G'$ for some idle F', G' by the induction hypothesis. Then

$$R, \mathscr{T}_{as}((fix_j \mathsf{Z}.\mathsf{H})[fix\,\mathsf{X}.\mathsf{F}/\mathsf{Y}]) \xrightarrow{a} \mu(a,R), G',$$

as required. □

We define the *contexts* $\mathscr{C}[-]$ of **ASCRP** in the standard way: a context is a process term of **ASCRP** but with multiple occurrences of a hole $[-]$ that may be plugged with any process term. We define a binary relation by

$$E \sim_{\mathrm{a}}^{\mathrm{c}} F \qquad \text{iff} \qquad \text{for all contexts } \mathscr{C}[-],\ \ \mathscr{T}_{as}(\mathscr{C}[E]) \sim_{\mathrm{a}} \mathscr{T}_{as}(\mathscr{C}[F])$$

for all **ASCRP**-processes E and F.

Proposition 59. For all **ASCRP**-processes E and F,

$$E \sim_{\mathrm{a}}^{\times} F \qquad \text{iff} \qquad E \sim_{\mathrm{a}}^{\mathrm{c}} F.$$

Proof. If $E \sim_{\mathrm{a}}^{\times} F$, then by Lemma 58, we have $\mathscr{C}[E] \sim_{\mathrm{a}}^{\times} \mathscr{C}[F]$ for every context $\mathscr{C}[-]$ of **ASCRP**. By Lemma 57, $\mathscr{T}_{as}(\mathscr{C}[E]) \sim_{\mathrm{a}} \mathscr{T}_{as}(\mathscr{C}[F])$ for every such context, so $E \sim_{\mathrm{a}}^{\mathrm{c}} F$.

If $E \sim_{\mathrm{a}}^{\mathrm{c}} F$, taking the context $[-] \times G$ for any agent G gives $\mathscr{T}_{as}(E \times G) \sim_{\mathrm{a}} \mathscr{T}_{as}(F \times G)$, so $E \sim_{\mathrm{a}}^{\times} F$. □

We write $E \sim_{\mathrm{a}}^{\mathrm{c}} F$ for any **ASCRP**-processes E and F with $\mathscr{T}_{as}(E) \sim_{\mathrm{a}}^{\mathrm{c}} \mathscr{T}_{as}(F)$.

Theorem 60. The following are equivalent for all processes E and F of **ASCRP**:

1 $E \sim_{\mathrm{a}}^{\mathrm{c}} F$.
2 $E \sim_{\mathrm{a}}^{\times} F$.
3 For all $a \in \mathsf{Act}$ and $R \in \mathbf{R}$:
   — if there is a transition $R, \mathscr{T}_{as}(E) \xrightarrow{a} \mu(a,R), E'$ for some E' in **SCRP**v, then $R, \mathscr{T}_{as}(F) \xrightarrow{a}\!\!\!\!\!\!\Longrightarrow^{\langle\rangle} \mu(a,R), F'$ for some F' in **SCRPr**v with $E' \sim_{\mathrm{a}} F'$;
   — if there is a transition $R, \mathscr{T}_{as}(F) \xrightarrow{a} \mu(a,R), F'$ for some F' in **SCRP**v, then $R, \mathscr{T}_{as}(E) \xrightarrow{a}\!\!\!\!\!\!\Longrightarrow^{\langle\rangle} \mu(a,R), E'$ for some E' in **SCRPr**v with $E' \sim_{\mathrm{a}} F'$.

Moreover, $\sim_{\mathrm{a}}^{\mathrm{c}}$ is a congruence, and if X contains all free variables of E and F, then $E \sim_{\mathrm{a}}^{\mathrm{c}} F$ if and only if $E[\mathsf{H}/\mathsf{X}] \sim_{\mathrm{a}}^{\mathrm{c}} F[\mathsf{H}/\mathsf{X}]$ for all tuples H of agents of **ASCRP** with the same length as X.

Proof. Parts 1 and 2 are equivalent by Proposition 59. Parts 2 and 3 are equivalent by Lemma 55. The relation $\sim_{\mathrm{a}}^{\mathrm{c}}$ is then a congruence by Lemma 58. The final property holds by Lemma 56. □

Corollary 61. If $E \sim_{\mathrm{a}} F$, then $a.E \sim_{\mathrm{a}}^{\mathrm{c}} a.F$.

5.3. *Asynchronous parallel composition*

Although the calculus **ASCRP** has captured a class of agents that are asynchronous (in the sense that all transitions are followed by idle states), it still contains a process constructor for synchronous, rather than asynchronous, parallel composition. For some

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

purposes **ASCRP** is still too powerful: if one takes a product of prefix processes, the resulting agent must perform both of the prefixed actions simultaneously. For example, at most an *ab*-transition is possible for any state of the form $R, \mathscr{T}_{as}((a.1) \times (b.1))$. We now introduce a further calculus **APSCRP** in which interleavings of such actions are allowed (but not forced) by a parallel composition. This is done by replacing the synchronous product $\times$ of **ASCRP** with an asynchronous parallel composition $|$.

The grammar of **APSCRP** is

$$E ::= X \mid a.E \mid \delta(E) \mid \sum_{i \in I} E_i \mid (E \mid E) \mid \nu R.E \mid fix_i \mathsf{X}.\mathsf{E}$$

where, the notation for variables and processes is as before, and this calculus is to be considered relative to a fixed $(\mathsf{Act}, \mathbf{R}, \mu, \nu)$. We then give a semantics to this calculus by translating into **SCRP**ν over the same $(\mathsf{Act}, \mathbf{R}, \mu, \nu)$. We define, by recursion, a translation $\mathscr{T}^0_{aps}$: **APSCRP** $\longrightarrow$ **ASCRP** by the clause

$$\mathscr{T}^0_{aps}(E \mid F) = (\mathscr{T}^0_{aps}(E) \times \delta(\mathscr{T}^0_{aps}(F))) + (\delta(\mathscr{T}^0_{aps}(E)) \times \mathscr{T}^0_{aps}(F))$$

together with clauses such that $\mathscr{T}^0_{aps}$ passes through the other process combinators in the evident way. Then we define a translation $\mathscr{T}_{aps}$: **APSCRP** $\longrightarrow$ **SCRP**ν as the composite map

$$\mathscr{T}_{aps} = \mathscr{T}_{as} \circ \mathscr{T}^0_{aps}.$$

The operational semantics is inherited from **SCRP**ν in a similar way to **ASCRP** using **SCRP**ν-transitions of the form

$$R, \mathscr{T}_{aps}(E) \xrightarrow{a} \mu(a, R), E'.$$

Lemma 62.

$$\mathscr{T}_{aps}(\delta(E \mid F)) \sim \mathscr{T}_{aps}(\delta(E) \mid F) \sim \mathscr{T}_{aps}(E \mid \delta(F)) \sim \mathscr{T}_{aps}(\delta(E)) \times \mathscr{T}_{aps}(\delta(F))$$

The proof of the above lemma is straightforward using Proposition 44.

Proposition 63. If $R, \mathscr{T}_{aps}(E) \xrightarrow{a} \mu(a, R), F$, then there is some agent E' of **APSCRP** such that $F \sim \delta(\mathscr{T}_{aps}(E'))$.

Proof. The proof is by induction on the inference of the given transition. Most cases are straightforward. The asynchronous product case uses Lemma 62. □

Note that in contrast to CCS, simultaneous actions are possible in **APSCRP** that are not pure synchronisations: compound actions are allowed. This is similar to the situation for the encoding of CCS in SCCS. In that case, however, one may sequentialise compound actions and so prove an appropriate (asynchronous) simulation between CCS processes and their encodings. Doing this for an **SCRP**-like calculus remains an open problem. The resource-based form of hiding we have adopted does not, in general, allow us to replace composite actions by a sequence of atomic actions corresponding to that composite.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

5.4. *Value passing*

In many process algebras, the ability to pass values into and out of processes is an important modelling mechanism – the first chapter of Milner (1989) contains an extended example. In this section we extend the asynchronous product language above with value-passing actions to give a calculus **APVSCRP**. This can be regarded as a collection of abbreviations (from **SCRP***v*) for efficiently expressing models of asynchronous situations with value passing. We allow atomic actions that simultaneously input and output values, in contrast to the standard treatment in CCS and SCCS (Milner 1980; 1983).

We assume a collection $\mathscr{V}$ of *values*, ranged over by v, that contains a set $\mathscr{B}$ of boolean values b including special values true and false. We assume a collection of (*value*) *variables* x, which should not be confused with the process variables. We assume a set $\mathscr{F}$ of *function symbols* f, each with a specified natural number, called the *arity*. We generate a set $\mathscr{E}$ of (*value*) *expressions* ϵ by

$$\epsilon ::= v \mid x \mid f(\epsilon_1, \ldots \epsilon_n)$$

where f is any function symbol of arity n, for any n. We assume that all expressions without variables evaluate to a unique value. For any expression ϵ containing no free variables, let v_ϵ be the value to which it evaluates. We write a vector of value variables as $\overline{x}$ and of expressions as $\overline{\epsilon}$.

The actions of the language are assumed to include atoms of the form

$$\alpha^{x_1,\ldots,x_m}_{\epsilon_1,\ldots,\epsilon_n}$$

for any integers $m, n \geqslant 0$ and sequences $\epsilon_1, \ldots, \epsilon_n$ and $x_1, \ldots, x_m$ of expressions and variables such that none of the x_i occurs free in any of the ϵ_j. The variables written as superscripts are said to be *inputs* to the action and the expressions written as subscripts are said to be *outputs*. Let ActV be the monoid that is freely generated from such actions.

We omit the superscripts when actions have no inputs, and the subscripts when actions have no outputs. In some situations only actions of the form $\alpha^{x_1,\ldots,x_m}$ and $\alpha_{\epsilon_1,\ldots,\epsilon_n}$ are required. We say that the former are *input actions* and the latter *output actions*, and in such situations we have essentially the standard form of value passing (as for CCS). Actions without parameters can be treated as special cases of outputs.

The grammar of **APVSCRP** is as follows:

$$E ::= a.E \mid \alpha^{\overline{x}}_{\overline{\epsilon}}.E \mid \sum_{i \in I} E_i \mid (E \mid E) \mid \nu R.E \mid A(x_1, \ldots, x_n) \mid \mathsf{if\ b\ then}\ E$$

where $a \in \mathsf{ActV}$ contains no input variables.

In a process $\alpha^{\overline{x}}_{\overline{\epsilon}}.E$, the input variables $\overline{x}$ are bound with scope E. The output variables $\overline{\epsilon}$ are not bound by this occurrence.

The process $\mathsf{if\ b\ then}\ E$ is a *conditional*. A conditional of the form $\mathsf{if\ b\ then}\ E_1\ \mathsf{else}\ E_2$ is definable by $(\mathsf{if\ b\ then}\ E_1) + (\mathsf{if}\ \neg\mathsf{b\ then}\ E_2)$ where $\neg$ is Boolean negation.

We write $E[a/\alpha]$ for the (capture-avoiding) result of replacing every occurrence of the free variable α in E by a. We write $E[\beta/\alpha]$ when α is of the form $\alpha_{\epsilon_1,\ldots,\epsilon_n}$ and we substitute $\beta_{\epsilon_1,\ldots,\epsilon_n}$ for α in E. We write $E[\epsilon/x]$ for the process that results from replacing every

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

APVSCRP	APSCRP
$\alpha^{x_1,\ldots,x_m}_{\epsilon_1,\ldots,\epsilon_n}.E \quad (\text{s.t. } 1 \leqslant m)$	$\sum_{(w_1,\ldots,w_m)\in\mathscr{V}^m} \alpha^{w_1,\ldots,w_n}_{v_{\epsilon_1},\ldots,v_{\epsilon_n}}.\mathscr{T}^0_{apv}(E[w_1/x_1,\ldots,w_n/x_n])$
$a.E$	$a.\mathscr{T}^0_{apv}(E)$ (where a contains no input variables)
$\sum_{i\in I} E_i$	$\sum_{i\in I}\ \mathscr{T}^0_{apv}(E_i)$
$E_1 \mid E_2$	$\mathscr{T}^0_{apv}(E_1) \mid \mathscr{T}^0_{apv}(E_2)$
$A(\epsilon_1,\ldots\epsilon_n)$	$A_{\epsilon_1,\ldots,\epsilon_n}$
if b then E	$\begin{cases}\mathscr{T}^0_{apv}(E) & \text{if } v_{\mathsf{b}} = \mathsf{true}\\ 0 & \text{otherwise}\end{cases}$

Fig. 9. Translation $\mathscr{T}^0_{apv}$

occurrence of the free input variable x appearing in E with the expression ϵ. We use the usual extension of this notation to simultaneous substitution for several distinct variables.

The process $A(x_1,\ldots,x_n)$ is a process *constant* with distinct value variables $x_1,\ldots,x_n$. We have chosen to use a process constant in order to be closer to the value-passing language of Milner (1989). Process constants are an alternative way of presenting fixed points: see Pym and Tofts (2006; 2007) for a discussion of this in **SCRP**. Constants are declared in families

$$\begin{aligned} A_1(x_1,\ldots,x_n) &= E_1\\ &\vdots\\ A_m(x_1,\ldots,x_n) &= E_m \end{aligned}$$

where the E_i are process terms of **APVSCRP** containing no free value variables except $x_1,\ldots,x_n$, no free agent variables and no constants other than those of this family.

We now show how to translate this value-passing calculus over ActV into an asynchronous fragment of **APSCRP** over another action monoid Act. We assume that Act contains every member of the family $(\alpha^{w_1,\ldots,w_m}_{v_1,\ldots,v_n} \mid v_i, w_j \in \mathscr{V})$ for each $\alpha^{x_1,\ldots,x_m}_{\epsilon_1,\ldots,\epsilon_n}$ in ActV, and every $a \in \mathsf{ActV}$ that contains no input variables.

The translation $\mathscr{T}^0_{apv}$ takes expressions of **APVSCRP** that contain no free value variables to processes in **APSCRP**. The clauses that recursively define this translation are given in Figure 9. The constant term $A_{\epsilon_1,\ldots,\epsilon_n}$ of **APSCRP** is defined to be the fixed-point expression $fix_i \mathsf{X}.\mathscr{T}^0_{apv}(\mathsf{E})$ for the appropriate i, where E is the tuple of declarations in which $A_{\epsilon_1,\ldots,\epsilon_n} = E_i$ was defined. We define the translation $\mathscr{T}_{apv}$ from **APVSCRP** to **SCRP**v to be the composite map $\mathscr{T}_{aps} \circ \mathscr{T}^0_{apv}$.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

As an example of the above translation $\mathscr{T}^0_{apv}$, consider the term

$$\alpha^x.\beta^y.\gamma_{x+y}.1$$

of **APVSCRP**. This translates as

$$\begin{aligned}\mathscr{T}^0_{apv}(\alpha^x.\beta^y.\gamma_{x+y}.1) &= \sum_{v\in\mathscr{V}} \alpha^v.\mathscr{T}^0_{apv}(\beta^y.\gamma_{v+y}.1)\\ &= \sum_{v\in\mathscr{V}} \alpha^v.\sum_{w\in\mathscr{V}} \beta^w.\mathscr{T}^0_{apv}(\gamma_{v+w}.1)\\ &= \sum_{v\in\mathscr{V}} \alpha^v.\sum_{w\in\mathscr{V}} \beta^w.\gamma_{v+w}.\mathscr{T}^0_{apv}(1)\\ &= \sum_{v\in\mathscr{V}} \alpha^v.\sum_{w\in\mathscr{V}} \beta^w.\gamma_{v+w}.1\end{aligned}$$

in **APSCRP**, which illustrates the difference between the inputs and outputs.

Once again, the calculus is closed under transitions up to $\sim$. The proof is essentially the same as that for Proposition 63, except that prefixes of atomic actions now translate as sums, so a transition of the translation of a value-passing prefix is one of the component transitions of the outermost sum.

Proposition 64. If E is an agent of **APVSCRP** and $R, \mathscr{T}_{apv}(E) \xrightarrow{a} \mu(a,R), E'$ for some R, then $E' \sim \delta(\mathscr{T}_{apv}(E''))$ for some agent E''.

It seems that in most situations mixed input–output actions are not required. Even where such mixed actions appear necessary, they can often be eliminated by extending the resource monoid to give temporary storage locations and replacing each mixed action with a pair of input and output actions that access the same cell in the temporary storage.

5.5. *A programming language*

It is possible to define parallel programming languages in the **SCRP** family of languages by an appropriate modification of Milner's technique for CCS. The idea is to translate the phrases of some programming language **P** into phrases of the process algebra. The language **P** then inherits a precise operational semantics from the process algebra. The translation of any program should capture the intended operational behaviour. Axioms for such intended behaviour, for example the associativity of parallel composition, should be validated by the appropriate asynchronous congruence of the process algebra. Examples of this for CCS can be found in Milner (1980; 1989). The example in Milner (1989) is a simple imperative programming language extended with parallelism and recursive, concurrent procedures. Thus the language allows a rather complicated form of shared-variable concurrency. In this sketch we do not do quite as much, for example, we omit the concurrent, recursive procedures.

The grammar of **P** is shown in Figure 10. The language includes value expressions ε, program variable declarations D and imperative commands C, including a parallel command `par`. The value expressions are formed from:

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

$$\varepsilon ::= \quad v \mid Y \mid F(\varepsilon, \ldots, \varepsilon)$$

$$C ::= \texttt{skip} \mid Y := \varepsilon \mid C; C' \mid \texttt{if } \varepsilon \texttt{ then } C \texttt{ else } C' \mid \texttt{while } \varepsilon \texttt{ do } C \mid C \texttt{ par } C' \mid \texttt{input } Y \mid \texttt{output } \varepsilon$$

Fig. 10. Syntax of **P**

— program variables Y;
— atomic values v (including integers) from a set *Vals*;
— a collection of function symbols F of given arity.

The main task in providing a translation for a programming language into a member of the **SCRP** family is to define, within the process algebra, appropriate structures and mechanisms for handling the flow of control and transfer of values from expressions to procedures. We use the the notation from the value-passing process calculus **APVSCRP** in conjunction with semaphore-like resources to make such definitions. Thus the calculus underpinning this work is **SCRP**v (with the more general notion of modification and the Hide-id rule, but without the side condition for piggybacking on the Hide rule), and the translation that defines the operational behaviour of terms written in the notation of **APVSCRP** takes terms into **SCRP**v. Note that here we are just using **APVSCRP** terms as a convenient macro notation for **SCRP**v terms.

The resource monoid **R** consists of triples (R^{st}, R^{sm}, R^{bu}) where the *store* R^{st} is a partial function from program variables to values R^{sm} is a partial function from a countable set *Sem* to the set $\{0,1\}$, and R^{bu} is a partial function from a set *Buff* to values. The components R^{sm} and R^{bu} represent the current states of sets of semaphores and value buffers. A resource R can be regarded as a partial map from the disjoint union of the sets of program variables, semaphores and buffers.

For any partial function f, let $dom(f)$ be the set of arguments of f at which f is defined. For any sets X, Y, partial function $f : X \longrightarrow Y$, $x \in X$ and $y \in Y$, we write $f \oplus \{f(x) = y\}$ for the partial function $g : X \longrightarrow Y$ such that $g(x) = y$ and for all $x' \in X$, we have $g(x') = f(x')$ if $f(x') \downarrow$ and $x' \neq x$, and $g(x') \uparrow$ if $f(x') \uparrow$ and $x' \neq x$. We write the empty partial map (from any source to any target) as $\varnothing$. A partial function $\varnothing_{x,y} : X \longrightarrow Y$ is defined for any sets X, Y and any $x \in X$, $y \in Y$ by taking $\varnothing_{x,y} = \varnothing \oplus \{\varnothing(x) = y\}$.

The set of stores is made into a resource monoid as follows. For each R^{st} and $R^{st\prime}$, the composite $R^{st} \circ R^{st\prime}$ is defined just when $dom(R^{st})$ is disjoint from $dom(R^{st\prime})$: the graph of $R^{st} \circ R^{st\prime}$ is then the union of the graphs of R^{st} and $R^{st\prime}$. The unit is $\varnothing$. The semaphores and buffers are made into resource monoids in a similar way. The resource monoid of interest is the product of the store, semaphore and buffer monoids: resource composition is given by

$$(R^{st}, R^{sm}, R^{bu}) \circ (R^{st\prime}, R^{sm\prime}, R^{bu\prime}) \simeq (R^{st} \circ R^{st\prime}, R^{sm} \circ R^{sm\prime}, R^{bu} \circ R^{bu\prime})$$

for all resources (R^{st}, R^{sm}, R^{bu}) and $(R^{st\prime}, R^{sm\prime}, R^{bu\prime})$. The unit resource is then $e = (\varnothing, \varnothing, \varnothing)$.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

$$\mu(\mathsf{in}^v, R) = \mu(\mathsf{out}_\varepsilon, R) = \mu(\mathsf{res}_\varepsilon, R) = \mu(\mathsf{done}, R) = R$$

$$\mu(\mathsf{ps}(i), R) = \begin{cases} R \oplus \{R^{sm}(i) = 0\} & \text{if } R^{sm}(i) = 1 \\ \uparrow & \text{otherwise} \end{cases}$$

$$\mu(\mathsf{pb}(i)^v, R) = \begin{cases} R \oplus \{R^{bu}(i) = 0\} & \text{if } R^{bu}(i) = v \\ \uparrow & \text{otherwise} \end{cases}$$

$$\mu(\mathsf{qs}(i), R)) = \begin{cases} R \oplus \{R^{sm}(i) = 1\} & \text{if } R^{sm}(i) \downarrow \\ \uparrow & \text{otherwise} \end{cases}$$

$$\mu(\mathsf{qb}(i)_v, R) = \begin{cases} R \oplus \{R^{bu}(i) = v\} & \text{if } R^{bu}(i) \downarrow \\ \uparrow & \text{otherwise} \end{cases}$$

$$\mu(\mathsf{get}(Y)^v, R) = \begin{cases} R & \text{if } R^{st}(Y) = v \\ \uparrow & \text{otherwise} \end{cases}$$

$$\mu(\mathsf{put}(Y)_v, R) = \begin{cases} R \oplus \{R^{st}(Y) = v\} & \text{if } R^{st}(Y) \downarrow \\ \uparrow & \text{otherwise} \end{cases}$$

Fig. 11. Modification function on atoms used for the translation of **P**

The action monoid for the value-passing calculus is freely generated from the actions

$$\mathsf{in}^x \qquad \mathsf{pb}(i)^x \qquad \mathsf{get}(Y)^x$$

and

$$\mathsf{out}_\varepsilon \qquad \mathsf{ps}(i) \qquad \mathsf{qs}(i) \qquad \mathsf{qb}(i)_\varepsilon \qquad \mathsf{put}(Y)_\varepsilon \qquad \mathsf{res}_\varepsilon \qquad \mathsf{done}$$

indexed by value variables x, value expressions $\varepsilon \in \mathscr{E}$, program variables Y and $i \in \mathbb{N}$. Notice that only input and output actions are required (and no mixed input–output actions).

There is a corresponding modification that ensures that:

— $\mathsf{qs}(i)$ increments and $\mathsf{ps}(i)$ decrements the ith semaphore;
— $\mathsf{qb}(i)_\varepsilon$ increments the ith buffer to hold the value corresponding to ε provided it currently holds 0;
— $\mathsf{pb}(i)^x$ sets the value in the ith buffer to 0, but note that because of the way values are passed, the value initially held in the ith buffer is bound to x in the process term;
— $\mathsf{put}(Y)_\varepsilon$ alters the store so that the memory allocated to the program variable Y holds the value corresponding to the expression ε;
— the action $\mathsf{get}(Y)^x$ retrieves the value stored at Y and binds it to x.

The definition of the modification on the corresponding atomic actions in Act for **SCRP**v is shown in Figure 11.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

The atomic actions have sets of roots as follows:

$$\mathsf{Roots}(\mathsf{in}^v) = \mathsf{Roots}(\mathsf{out}_v) = \mathsf{Roots}(\mathsf{res}_v) = \mathsf{Roots}(\mathsf{done}) = \{e\}$$

$$\mathsf{Roots}(\mathsf{get}(Y)^v) = \{(\varnothing_{Y,v}, \varnothing, \varnothing)\}$$

$$\mathsf{Roots}(\mathsf{put}(Y)_v) = \{(\varnothing_{Y,w}, \varnothing, \varnothing) \mid w \in \mathbb{N}\}$$

$$\mathsf{Roots}(\mathsf{ps}(i)) = \{(\varnothing, \varnothing_{i,1}, \varnothing)\}$$

$$\mathsf{Roots}(\mathsf{qs}(i)) = \{(\varnothing, \varnothing_{i,0}, \varnothing)\}, (\varnothing, \varnothing_{i,1}, \varnothing)\}$$

$$\mathsf{Roots}(\mathsf{pb}(i)^v) = \{(\varnothing, \varnothing, \varnothing_{i,v})\}$$

$$\mathsf{Roots}(\mathsf{qb}(i)_v) = \{(\varnothing, \varnothing, \varnothing_{i,w}) \mid w \in \mathbb{N}\}.$$

By Proposition 22, this defines a modification. The family is coherent because composition works as non-overlapping union.

The atomic value expressions are given a semantics as processes in the asynchronous value-passing calculus in such a way that every translation issues an action res_v for a unique value v immediately before it terminates, if it terminates, and no earlier. For atomic expressions this is done as follows:

$$[\![v]\!] = \mathsf{res}_v.0 \qquad [\![Y]\!] = \mathsf{get}(Y)^x.\mathsf{res}_x.0$$

where v is not a program variable. Complex expressions have the form $F(\varepsilon_1, \ldots, \varepsilon_n)$ where each ε_i is an expression and F is an n-ary function symbol of the programming language. Each such function symbol is assumed to be tracked by a given n-ary function f on the set of values. We then define

$$[\![F]\!] = \mathsf{pb}(1)^{x_1}.\cdots.\mathsf{pb}(n)^{x_n}.\mathsf{res}_{f(x_1,\ldots,x_n)}.0$$

for function symbols. The application is defined by

$$[\![F(\varepsilon_1, \ldots, \varepsilon_n)]\!] = \nu(R_1 \circ \ldots \circ R_n).([\![\varepsilon_1]\!][\mathsf{qb}(1)/\mathsf{res}] \mid \ldots \mid [\![\varepsilon_n]\!][\mathsf{qb}(n)/\mathsf{res}] \mid [\![F]\!])$$

where each resource R_i mentioned has $R_i = (\varnothing, \varnothing, R_i^{bu})$ and the R_i^{bu}, $\mathsf{qb}(i)$, $\mathsf{pb}(i)$ are distinct from all other buffers used within the term. In particular, $R_i^{bu}(j)$ is defined for a unique j, say j_i, and $R_i^{bu}(j_i) = 0$, and $R_k^{bu}(j_i) \uparrow$ for all $1 \leqslant i, k \leqslant n$ and $k \neq i$. This definition is not compatible with the piggybacking restriction on hiding from **SCRPr***v*.

We now turn to the denotation of commands. Processes used to denote commands are constructed in such a way that they send out an action done before terminating, if they terminate, and these actions occur only immediately prior to termination.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

$$[\![Y := \varepsilon]\!] = [\![\varepsilon]\!]\ \mathit{Into}(x)\ \mathsf{put}(Y)_x.\ \mathit{Done}$$

$$[\![C\,;C']\!] = [\![C]\!]\ \mathit{Before}\ [\![C']\!]$$

$$[\![\texttt{if}\ \varepsilon\ \texttt{then}\ C\ \texttt{else}\ C']\!] = [\![\varepsilon]\!]\ \mathit{Into}(x)\ (\mathsf{if}\ x\ \mathsf{then}\ [\![C]\!]\ \mathsf{else}\ [\![C']\!])$$

$$[\![\texttt{while}\ \varepsilon\ \texttt{do}\ C]\!] = W\ ,\ \text{where}\ W = [\![\varepsilon]\!]\ \mathit{Into}(x)\ (\mathsf{if}\ x\ \mathsf{then}\ ([\![C]\!]; W)\ \mathsf{else}\ \mathit{Done})$$

$$[\![C\ \texttt{par}\ C']\!] = [\![C]\!]\ \mathit{Par}\ [\![C']\!]$$

$$[\![\texttt{input}\ Y]\!] = \mathsf{in}^x.\mathsf{put}(Y)_x.\ \mathit{Done}$$

$$[\![\texttt{output}\ \varepsilon]\!] = [\![\varepsilon]\!]\ \mathit{Into}(x)\ (\mathsf{out}_x.\ \mathit{Done})$$

$$[\![\texttt{skip}]\!] = \ \mathit{Done}$$

Fig. 12. Semantics of commands of **P**

We define auxiliary control operators as follows:

$$\mathit{Done} \ = \ \mathsf{done}.0$$

$$E\ \mathit{Before}\ F \ = \ \nu R_i.(E[\mathsf{qs}(i)/\mathsf{done}] \mid \mathsf{ps}(i).F)$$

$$E\ \mathit{Par}\ F \ = \ \nu(R_i \circ R_j).\ (E[\mathsf{qs}(i)/\mathsf{done}] \mid F[\mathsf{qs}(j)/\mathsf{done}] \mid (\mathsf{ps}(i).\mathsf{ps}(j).\ \mathit{Done} + \mathsf{ps}(j).\mathsf{ps}(i).\ \mathit{Done} + \mathsf{ps}(i)\mathsf{ps}(j).\ \mathit{Done}))$$

$$E\ \mathit{Into}(x)\ F \ = \ \nu R_k.(E[\mathsf{qb}(k)/\mathsf{res}] \mid \mathsf{pb}(k)^x.F)$$

where R_i and R_j each represent fresh semaphores (unused by actions in E and F) initialised to 0. In particular, $R_i = (\varnothing, R_i^{sm}, \varnothing)$ with $R_i^{sm}(n)$ defined for a unique $n = n_i$, and with $R_i^{sm}(n_i) = 0$. The process *Done* is a simple terminating process. The combinator *Before* is used to sequence processes. This is done by ensuring that E increments the semaphore R_i (using $\mathsf{qs}(i)$) immediately before termination, if that happens, and that the semaphore must be decremented (using $\mathsf{ps}(i)$) before F begins. The combinator *Par* is used to parallel compose processes. The term $\mathsf{ps}(i)\mathsf{ps}(j).\ \mathit{Done}$ is necessary in *Par* because the parallel process combinator | allows for the possibility that E and F complete in synchrony. The combinator $\mathit{Into}(x)$ takes a process E that outputs a value and transfers this value into a second process F through the private, mediating buffer R_k. The resource R_k represents a fresh buffer with $R_k = (\varnothing, \varnothing, R_k^{bu})$, with $R^{bu}{}_k(n)$ defined for a unique $n = n_k$, and with $R_k^{bu}(n_k) = v$, where v is the value signalled by the output res_v of E.

The semantics of commands is given in Figure 12.

Let $R_0 = (R_0^{st}, \varnothing, \varnothing)$ be the resource with $R_0^{st}(Y) = 0$ for all program variables Y. A program of **P** is taken to be a command C. The behaviour of C is then determined by the operational behaviour of the translation of $[\![C]\!]$ into **SCRP**v, considered in the

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

$$\varepsilon ::= \quad \ldots \mid \varepsilon.i$$

$$C ::= \ldots \mid Y := \varepsilon.i \mid \varepsilon.i := \varepsilon' \mid Y := \texttt{cons}(\varepsilon, \varepsilon')$$
$$\mid \texttt{dispose}(\varepsilon) \mid \texttt{with } i \texttt{ when } \varepsilon \texttt{ do } C \texttt{ endwith}$$

Fig. 13. Syntax of commands of **PH**

environment R_0. Thus, if $\mathscr{T}_{apv}$ is the translation from the asynchronous value-passing notation into **SCRP**v, then the semantics of the program is determined by transitions of $R_0, \mathscr{T}_{apv}([\![C]\!])$.

The above method can be extended to allow block commands of the form

$$\texttt{begin } D \texttt{ ; } C \texttt{ end}$$

containing local variable declarations of the form $D ::= \texttt{Var } Y$. A semantics can then be given by first extending the domain of the store component of each resource R with a disjoint countable set $TVar$ of temporary variables, giving a partial function $R^{st} : GVar \cup TVar \longrightarrow Vals$, where $GVar$ is the set of global variables. We then extend the definition of μ so that the Y in $\mathsf{put}(Y)_v$ and $\mathsf{get}(Y)^v$ ranges over both global and temporary variables. We then take

$$[\![\texttt{Var } Y ; C]\!] = \nu R_{Y'}.[\![C]\!][Y'/Y]$$

where Y' is a fresh temporary variable, which we substitute for Y, and the resource $R_{Y'} = (R^{st}_{Y'}, \varnothing, \varnothing)$, with $R^{st}_{Y'}(X) = 0$ if $X = Y'$, and $R^{st}_{Y'}$ is undefined for all other global and temporary variables X. Localisation of variables is then realised as an instance of hiding. We have not attempted to extend the method to allow for procedure declarations in D.

5.6. *Heap manipulating commands*

We form a language **PH** by adding commands for manipulating pointers to **P**. These commands are similar to those found in languages used to illustrate Concurrent Separation Logic (O'Hearn 2007). In particular, the language has commands for assignment from a heap cell, update of a heap cell, pointer creation and pointer disposal, and conditional critical regions that are protected by semaphores.

The set of values is extended to include a countable set Loc of locations, ranged over by l. The extensions to the syntax are shown in Figure 13. Note that locations are expressions. The expression $\varepsilon.i$ extracts the ith component of a location defined by ε, and is undefined if ε does not evaluate to a location. The command $Y := \varepsilon.i$ stores the contents of $\varepsilon.i$ at the global variable Y. The command $\varepsilon.i := \varepsilon'$ sets the contents of $\varepsilon.i$ to the value of ε'. The command $Y := \texttt{cons}(\varepsilon, \varepsilon')$ inserts the values ε and ε' at some fresh location l and stores the value l at the global variable Y. The command $\texttt{dispose}(\varepsilon)$ removes the location ε from the heap. The command $\texttt{with } i \texttt{ when } \varepsilon \texttt{ do } C \texttt{ endwith}$ executes the command C when both ε evaluates to true and the ith semaphore is free; the command C then owns the

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

*i*th semaphore whilst executing, and the disjointness condition on semaphores in resource composition means that no other command that requires the *i*th semaphore can make progress whilst C does.

Resources R now take the form $(R^{st}, R^{sm}, R^{bu}, R^{hp})$ where the store, semaphore and buffer components are as before and the *heap* R^{hp} is a partial function from Loc to pairs of values (said, conventionally, to be contained in cells). The heap R^{hp} is assumed to be finite in the sense that it is defined at only finitely many locations. We write $R^{hp}(l)(j)$ for the jth component of the pair at location l. Note that pointers can be stored at program variables and in cells because the set of values contains locations. The composite of two resources is defined just when the stores, semaphores, buffers and heaps defined at one resource are disjoint from the stores, semaphores, buffers and heaps defined at the other resource: under such circumstances it is defined by the union of graphs.

To the atomic actions above, we add

$$\mathsf{rem}_{\varepsilon} \qquad \mathsf{alloc}_{\varepsilon} \qquad \mathsf{puth}(i)_{\varepsilon,\varepsilon'} \qquad \mathsf{geth}(i)^{x}_{\varepsilon},$$

where $i = 1, 2$, to the set of atomic actions and generate a new action monoid. Note that mixed input–output actions (of the form $\mathsf{geth}(i)^{x}_{\varepsilon}$) are now present.

For any partial function $f : X \longrightarrow Y$ and $x \in X$, we define $f \ominus x : X \longrightarrow Y$ by $f \ominus x(x') \simeq f(x')$ if $x' \neq x$ and $f \ominus x(x) \uparrow$.

The modification μ is chosen so that:

— the action $\mathsf{puth}(i)_{\varepsilon,\varepsilon'}$ puts the value ε' at the ith component of the cell at location ε;

— the action $\mathsf{geth}(i)^{x}_{\varepsilon}$ retrieves the value stored at the ith component of the cell at location ε and binds it to x;

— the action $\mathsf{alloc}_{\varepsilon}$ is used in the allocation of a location ε, and is undefined if the location is not fresh;

— the action $\mathsf{rem}_{\varepsilon}$ removes the heap cells at location $[\![\varepsilon]\!]$.

In each of these, the expression ε must evaluate to some location, otherwise the modification is undefined at every resource. The extensions of the modification to the new atomic actions is shown in Figure 14. It is worth noting that the action of the modification at alloc_{v} is incompatible with the simple-extension property, so we use **SCRP***v* rather than **SCRPr**.

The roots of the atomic actions are as follows:

$$\mathsf{Roots}(\mathsf{rem}_{v}) = \{(\varnothing, \varnothing, \varnothing, \varnothing_{v,w}) \mid w \in \mathit{Vals} \times \mathit{Vals}\}$$

$$\mathsf{Roots}(\mathsf{alloc}_{v}) = \{e\}$$

$$\mathsf{Roots}(\mathsf{puth}(j)_{v,w}) = \{(\varnothing, \varnothing, \varnothing, \varnothing_{v,v'}) \mid v' \in \mathit{Vals} \times \mathit{Vals}\}$$

$$\mathsf{Roots}(\mathsf{geth}(j)^{w}_{v}) = \{(\varnothing, \varnothing, \varnothing, \varnothing_{v,v'}) \mid v' \in \mathit{Vals} \times \mathit{Vals} \text{ and } v'(j) = w\}.$$

The modification that follows from the data in Figure 14 is then defined as in Proposition 22.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

$$\mu(\mathsf{rem}_v, R) = \begin{cases} (R^{st}, R^{sm}, R^{bu}, R^{hp} \ominus v) & \text{if } R^{hp}(v) \downarrow \\ \uparrow & \text{otherwise} \end{cases}$$

$$\mu(\mathsf{alloc}_v, R) = \begin{cases} R \oplus \{R^{hp}(v) = (0,0)\} & \text{if } R^{hp}(v) \uparrow \text{ and } v \in Loc \\ \uparrow & \text{otherwise} \end{cases}$$

$$\mu(\mathsf{puth}(j)_{v,w}, R) = \begin{cases} R \oplus \{R^{hp}(v)(j) = w\} & \text{if } R^{hp}(v) \downarrow \\ \uparrow & \text{otherwise} \end{cases}$$

$$\mu(\mathsf{geth}(j)^w_v, R) = \begin{cases} R & \text{if } R^{hp}(v)(j) = w \text{ and } v \in Loc \\ \uparrow & \text{otherwise} \end{cases}$$

Fig. 14. Modification function on atoms for heap manipulation

$$[\![Y := \varepsilon.i]\!] = [\![\varepsilon.i]\!]\ \mathit{Into}(x)\ (\mathsf{put}(Y)_x.\ \mathit{Done})$$

$$[\![\varepsilon.i := \varepsilon']\!] = [\![\varepsilon]\!]\ \mathit{Into}(z)\ ([\![\varepsilon']\!]\ \mathit{Into}(x)\ (\mathsf{puth}(i)_{z,x}.\ \mathit{Done}))$$

$$[\![\texttt{dispose}(\varepsilon)]\!] = \mathsf{rem}_{[\![\varepsilon]\!]}.\ \mathit{Done}$$

$$[\![\texttt{with}\ i\ \texttt{when}\ \varepsilon\ \texttt{do}\ C\ \texttt{endwith}]\!] = \nu(\varnothing, \varnothing_{i,1}, \varnothing, \varnothing).\ \text{if } [\![\varepsilon]\!] \text{ then } [\![C]\!]$$

$$[\![Y := \texttt{cons}(\varepsilon, \varepsilon')]\!] = [\![\varepsilon'[y/x]]\!]\ \mathit{Into}(y)\ ([\![\varepsilon]\!]\ \mathit{Into}(x)\ A(x,y)), \text{ where}$$

$$A(x,y) = \textstyle\sum_{l \in Loc} \mathsf{alloc}_l.\mathsf{put}(Y)_l.\mathsf{puth}(1)_{l,x}.\mathsf{puth}(2)_{l,y}.\ \mathit{Done}$$

Fig. 15. Semantics of commands of **PH**

We extend the above semantics of expressions to translate the components of expressions that evaluate to locations by taking

$$[\![\varepsilon.i]\!] = [\![\varepsilon]\!]\ \mathit{Into}(z)\ \mathsf{geth}(i)^x_z.\mathsf{res}_x.0$$

for $i = 1, 2$. The extension of the semantics of commands is in Figure 15. The resource $(\varnothing, \varnothing_{i,1}, \varnothing, \varnothing)$ represents the ith semaphore (set to 1).

Milner evaluated his translation of a programming language into CCS by proving that the intended algebraic and logical structure of programs holds in the translation. It remains an open problem to define a calculus in the **SCRP** family for which a well-behaved asynchronous equivalence exists, and in which one may prove the expected program equivalences using a semantics of **P** or **PH** in the above style. We anticipate a close connection between the Hennessy–Milner logic **MBIc** in this context and Concurrent Separation Logic (O'Hearn 2007), which is a Floyd–Hoare logic with a **BI**-fragment as assertion language. Given a translation of the programming language

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

into a **SCRP**-calculus, any triple $\{\phi\}C\{\psi\}$ corresponds to an assertion of the form $\phi \longrightarrow \bigwedge_{a_1 \ldots a_n \in \mathscr{A}(\llbracket C \rrbracket)}([a_1] \ldots [a_n]\psi)$, where $\mathscr{A}(\llbracket C \rrbracket)$ is the (finite) set of all finite sequences of actions that the translated process $\llbracket C \rrbracket$ can make. It would therefore be interesting to see whether the Concurrent Separation Logic rules can be derived from our logic.

6. Future directions

There are a great many open problems and possible avenues for future research in this area. In this section, we outline a few of these.

The process constructors of **SCRP** seem natural, and appear to be sufficiently powerful for the description of many (if not most) concurrent situations. We have not, however, yet proved any kind of completeness result. This could, perhaps, be done by either proving a result along the lines of de Simone(1985), or by finding a suitable resource monoid such that there is a well-behaved translation of SCCS into **SCRP**. Equally, it would be very interesting to see if the process constructors we have defined emerge naturally as universal constructions in a fibred category following the methodology described in Winskel and Nielsen (1995). It may be that a presheaf semantics for SCCS (Hildebrandt 1999) may also have useful connections – sheaves and presheaves can be used to interpret multiplicative conjunction (Pym 2002). Such approaches would also be helpful in assessing the value of further rules.

The availability of good model-checking procedures has been fundamental for the successful application of process algebras and modal logics. Preliminary work has been done on implementing prototype systems for the automatic construction of **SCRP**-transitions and for model-checking formulae of **MBI**. Recall that the general model-checking problem is to decide whether a given state satisfies a given formula. We note that the model-checking problem for the whole of **SCRP** and **MBIc** is much harder than traditional model checking for process algebras. The essential difference is that multiplicative formulae demand that subformulae must be checked against states that are outside the transition structure generated by the given state. In particular, this involves unbounded searches across infinite sets of states. Strategies for bounding such searches, such as the use of the underlying order and properties of the modification function, will be critical to establishing better algorithms.

The model checking of the multiplicative conjunction raises another issue. In order to check that some relation $R, E \vDash \phi_1 * \phi_2$ is satisfied, it is necessary to find R_1, R_2, E_1 and E_2 with $R = R_1 \circ R_2$, $E \sim E_1 \times E_2$, $R_1, E_1 \vDash \phi_1$ and $R_2, E_2 \vDash \phi_2$. In general, the global bisimulation will not be decidable. An alternative is to use the structural congruence $\equiv$ between processes. This is the congruence generated from associativity, commutativity and unit axioms for the sum and product constructors. These axioms are all true for global bisimulation when the frame rule is admissible (that is, the simple-extension property for transitions holds), so the global bisimulation must contain the structural congruence. The structural congruence is decidable, so a better alternative for the interpretation of multiplicative conjunction might be to use: $R, E \vDash \phi_1 * \phi_2$ if and only if $\exists R_1, R_2, E_1, E_2.\ R = R_1 \circ R_2$ and $E \equiv E_1 \times E_2$ and $R_1, E_1 \vDash$

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

ϕ_1 and $R_2, E_2 \vDash \phi_2$ for all R, E, ϕ_1, ϕ_2. Now suppose we also change the interpretation of the multiplicative unit to $R, E \vDash I$ iff $R = e$ and $E \equiv \mathsf{1}$, for all R, E. Then:

— Theorem 26 holds with $\equiv$ in place of $\sim$.

— The axioms of **BI** are all soundly interpreted.

We intend to investigate this promising avenue of further research, in particular, for model checking. We note that Cardelli and Gordon (1998) also contains a version of multiplicative conjunction, written |, which is interpreted by splitting processes using a structural congruence.

It appears that the boundedness and convergence properties of modifications will be of help in dealing with some of these model-checking problems. They may also be the kind of properties that we wish to check. To this end, we have constructed a version of **SCRP** that works over a topological, rather than ordered, resource space and have shown how to interpret **MBIi** as open sets of a space induced on states. However, this requires placing certain continuity conditions on **SCRP** constructors, and we still need to evaluate the practicality of the approach. This work dovetails rather well with our goal of studying the relationship between process algebras and other mathematical models of dynamical systems. In connection with this, we have also produced some preservation results for dynamical and logical properties under transformation of the resource base. We imagine that this will have applications to the study of data refinement.

Open problems exist with regard to establishing precise correspondences between the algebraic notions of equivalence (simulations) and logical equivalence. Is there a logic that characterises the relation $\sim$, at least on some reasonable class of resource monoids? Alternatively, is there a simulation relation bigger than $\sim$, but smaller than $\approx$, such that suitable versions of Theorem 26 and Theorem 35 both hold for that simulation and for the whole language **MBI**?

The questions of completeness of the interpretation of **MBIc**, **MBIq** and of the equational theory of $\sim$ all remain open.

A good question is what the relation $\sim$ is for from an operational (rather than logical) point of view given that $\approx$ characterises observational and denotational equivalence (Pym and Tofts 2007; Collinson *et al.* 2007). In many modelling situations, resources are real-valued quantities. In such situations, evolutions may be dependent upon functions that have rather wild behaviour. It is important to understand, and be able to make guarantees about, the stability properties of such functions under small perturbations. There is a great deal of literature on this topic, but, for example, the recent paper Hoyrup (2007) studies various notions of stability and computability with a view to understanding those systems that admit reliable computer simulations. A careful reading of Example 34 shows that the logical connectives $\langle a \rangle$ and $-\!\!*$ make assertions about perturbations of the resource component during the evolution of the state. The relation $\sim$ can be seen to identify processes that have equivalent behaviour under all such perturbations of states that occur during the evolution. We still need to evaluate the extent to which **SCRP**, **MBI** and $\sim$ (or topological variants thereof) are practical modelling tools for problems in this area.

We have presented proof systems for variants of **MBI**, but have not considered the completeness of these proof systems with respect to their transition structure semantics.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

Indeed, since we are concerned only with one particular underlying structure, namely that generated by **SCRP**-transitions for each choice of $(\mathbf{R}, \mathsf{Act}, \mu, \nu)$, a complete axiomatisation may be difficult. We have so far paid little attention to proof-theoretic aspects of **MBI**, for example, cut elimination. The problem of finding decision procedures for this logic is particularly important because of the difficulties involved in model checking. A full analysis of the logical rules and models for multiplicative quantification still needs to be worked out. We expect that the models should be instances of (pre)sheaf models of predicate modal logic and that our previous work on multiplicative quantification (O'Hearn and Pym 1999; Pym 1999; 2002; Collinson *et al.* 2008) should provide some guidelines.

Further developments of the process calculus should also prove valuable. The addition of weights on actions (for priority and probabilistic distribution) along the lines of Tofts (1994) is essential if the calculus is to be developed into a mature and sufficiently expressive modelling tool. We have begun a further refinement of the calculus to one in which states carry a component signifying location. This location is intended as an additional guard against action, but will evolve in a different way to resources in most of the modelling situations we have in mind. In particular, practical modelling work suggests that such an explicit notion of location would be of use in describing certain security properties of large-scale distributed systems.

Acknowledgements

We are grateful to Chris Tofts, who declined to be named as an author, for his input to this work, to Matthew Hennessy and the anonymous referees for raising questions that led to significant corrections. Example 6 was suggested by one of the referees. We are also grateful to Brian Monahan and Mike Yearworth for their support.

References

Baeten, J. (2005) A brief history of process algebra. *Theoretical Computer Science* **335** (2-3) 131–146.

Ben-Ari, M. (1990) *Principles of Concurrent and Distributed Programming*, Prentice Hall.

Biri, N. and Galmiche, D. (2007) Models and separation logics for resource trees. *Journal of Logic and Computation* **17** (4) 687–726.

Birtwistle, G. (1979) *Demos – discrete event modelling on Simula*, Macmillan.

Birtwistle, G., Pooley, R. and Tofts, C. (1993) Characterising the structure of simulations using CCS. *Transactions of the Simulation Society* **10** (3) 205–236.

Birtwistle, G. and Tofts, C. (2001a) Getting Demos models right. (i). Practice. *Simulation Practice and Theory* **8** (6-7) 377–393.

Birtwistle, G. and Tofts, C. (2001b) Getting Demos models right. (ii)…and theory. *Simulation Practice and Theory* 8 (6-7) 395–414.

Calcagno, C., Gardner, P. and Zarfaty, U. (2005) Context logic and tree update. In: *Proceedings of the 32nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages 2005 (POPL)* 271–282.

Cardelli, L. and Gordon, A. (1998) Mobile ambients. In Nivat, M. (ed.) Foundations of Software Science and Computational Structures. *Springer-Verlag Lecture Notes in Computer Science* **1378** 40–155.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

Cleaveland, R., Parrow, J. and Steffen, B. (1993) The Concurrency Workbench: a semantics based tool for the verification of concurrent systems. In *ACM Transactions on Programming Languages and Systems* **15** 36–72.

Collinson, M., Pym, D. and Robinson, E. (2008) Bunched Polymorphism. *Mathematical Structures in Computer Science* **18** 1091–1132.

Collinson, M., Pym, D. and Tofts, C. (2007) Errata for Formal Aspects of Computing (2006) **18** 495–517 and their consequences. *Formal Aspects of Computing* **19** (4) 551–554.

Conforti, G., Macedonio, D. and Sassone, V. (2007) Static bilog: a unifying language for spatial structures. *Fundamenta Informaticae* **80** 1–20.

Dahl, O.-J., Myhrhaug, B. and Nygaard, K. (1970) Simula 67 Common Base Language. NCC Publication S-52, Norwegian Computing Center, Oslo.

Day, B. (1970) On closed categories of functors. In Proceedings of the Midwest Category Seminar. *Springer-Verlag Lecture Notes in Mathematics* **137**.

Day, B. (1973) An embedding theorem for closed categories. In: Proceedings of the Sydney Category Seminar 1972/73. *Springer-Verlag Lecture Notes in Mathematics* **420**.

Demos 2k Team (2002) Demos 2000. `http://www.demos2k.org`.

de Simone, R. (1985) Higher-level synchronising devices in Meije-SCCS. *Theoretical Computer Science* **37** 245–267.

Hennessy, M. and Milner, R. (1985) Algebraic laws for nondeterminism and concurrency. *Journal of the ACM* **32** (1) 137–161.

Hildebrandt, T. (1999) A Fully Abstract Presheaf Semantics of SCCS with Finite Delay. In: Proceedings of CTCS'99. *Electronic Notes in Theoretical Computer Science* **29**.

Hinton, A., Kwiatkowska, M., Norman, G. and Parker, D. (2006) Prism: A tool for automatic verification of probabilistic systems. In: Hermanns, H. and Palsberg, J. (eds.) Proc. 12th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'06). *Springer-Verlag Lecture Notes in Computer Science* **3920** 441–444.

Hoyrup, M. (2007) Dynamical systems: stability and simulability. *Mathematical Structures in Computer Science* **17** (2) 247–259.

Ishtiaq, S. and O'Hearn, P. (2001) BI as an assertion language for mutable data structures. In: *Proceedings of the 28th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages 2001 (POPL), London* 14–26.

Joyal, A., Nielsen, M. and Winskel, G. (1996) Bisimulation from open maps. *Information and Computation* **127** 164–185.

Kripke, S. (1963) Semantical analysis of modal logic I. *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik* **9** 67–96.

Kripke, S. (1965) Semantical analysis of intutionistic logic I. In: Crossley, J. and Dummett, M. (eds.) *Formal Systems and Recursive Functions*, Studies in Logic and the Foundations of Mathematics, North-Holland 92–130.

Lawvere, F. (1969) Adjointness in foundations. *Dialectica* **23** 281–296.

Leifer, J. J. and Milner, R. (2000) Deriving bisimulation congruences for reactive systems. In: Proc. CONCUR 2000. *Springer-Verlag Lecture Notes in Computer Science* **1877**.

Milner, R. (1980) A Calculus of Communicating Systems. *Springer-Verlag Lecture Notes in Computer Science* **92**.

Milner, R. (1983) Calculi for synchrony and asynchrony. *Theoretical Computer Science* **25** 267–310.

Milner, R. (1989) *Communication and Concurrency*, Prentice-Hall.

Milner, R. (1999) *Communicating systems and the π-calculus*, Cambridge University Press.

O'Hearn, P. (2007) Resources, concurrency and local reasoning. *Theoretical Computer Science* **375** (1-3) 271–307.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press

O'Hearn, P. and Pym, D. (1999) The logic of bunched implications. *Bulletin of Symbolic Logic* **5** (2) 215–244.

Plotkin, G. (2004) Structural operational semantics. *Journal of Logic and Algebraic Programming* **60** 17–139. (Original unpublished manuscript 1981.)

Popkorn, S. (1994) *First Steps in Modal Logic*, Cambridge University Press.

Pym, D. (1999) On bunched predicate logic. In: *Proceedings of the 14th Symposium on Logic in Computer Science (LICS99), Trento, Italy*, IEEE Computer Society Press 183–192.

Pym, D. (2002) *The Semantics and Proof Theory of the Logic of Bunched Implications*, Applied Logic Series **26**, Kluwer Academic Publishers. (Errata at: `http://www.cs.bath.ac.uk/~pym/BI-monograph-errata.pdf`.)

Pym, D., O'Hearn, P. and Yang, H. (2004) Possible worlds and resources: The semantics of **BI**. *Theoretical Computer Science* **315** (1) 257–305.

Pym, D. and Tofts, C. (2006) A calculus and logic of resources and processes. *Formal Aspects of Computing* **18** (4) 495–517. (Errata available: `http://www.cs.bath.ac.uk/~pym/pym-tofts-fac-errata.pdf`.)

Pym, D. and Tofts, C. (2007) Systems Modelling via Resources and Processes: Philosphy, Calculus, Semantics, and Logic. In: Cardelli, L., Fiore, M. and Winskel, G. (eds.) Computation, Meaning and Logic: articles dedicated to Gordon Plotkin. *Electronic Notes in Theoretical Computer Science* **172** 545–587. (Errata at: `http://www.cs.bath.ac.uk/~pym/pym-tofts-fac-errata.pdf`.)

Reynolds, J. (2002) Separation logic: a logic for shared mutable data structures. In: *Proceedings of the 17th Annual IEEE Symposium on Logic in Computer Science (LICS02), Copenhagen, Denmark*, IEEE Press 55–74.

Sassone, V. and Sobociński, P. (2003) Deriving bisimulation congruences using 2-categories. *Nordic Journal of Computing* **10** 163–183.

Sewell, P. (1998) From rewrite rules to bisimulation congruences. *Springer-Verlag Lecture Notes in Computer Science* **1466** 269–284.

Stirling, C. (2001) *Modal and temporal properties of processes*, Springer-Verlag.

Tofts, C. (1994) Processes with probabilities, priority and time. *Formal Aspects of Computing* **6** 536–564.

Tofts, C. (2006) Process algebra as modelling. In: Proceedings of the Workshop 'Essays on Algebraic Process Calculi' (APC25). *Electronic Notes in Theoretical Computer Science* **162** 323–326.

Victor, B. and Moller, F. (1994) The Mobility Workbench – a tool for the π-calculus. In: Dill, D. (ed.) CAV'94: Computer Aided Verification. *Springer-Verlag Lecture Notes in Computer Science* **818** 428–440.

Winskel, G. and Nielsen, M. (1995) Models for concurrency. In: *Handbook of Logic in Computer Science* **4**, Oxford University Press 1–148.

https://doi.org/10.1017/S0960129509990077 Published online by Cambridge University Press