From Rewrite Rules to Bisimulation Congruences

Peter Sewell

Computer Laboratory, University of Cambridge,
New Museums Site, Pembroke Street, Cambridge, CB2 3QG.
Peter.Sewell@cl.cam.ac.uk

Abstract

The dynamics of many calculi can be most clearly defined by a reduction semantics. To work with a calculus, however, an understanding of operational congruences is fundamental; these can often be given tractable definitions or characterisations using a labelled transition semantics. This paper considers calculi with arbitrary reduction semantics of three simple classes, firstly ground term rewriting, then left-linear term rewriting, and then a class which is essentially the action calculi lacking substantive name binding. General definitions of labelled transitions are given in each case, uniformly in the set of rewrite rules, and without requiring the prescription of additional notions of observation. They give rise to bisimulation congruences. As a test of the theory it is shown that bisimulation for a fragment of CCS is recovered. The transitions generated for a fragment of the Ambient Calculus of Cardelli and Gordon, and for SKI combinators, are also discussed briefly.

Key words: Operational Semantics, Process Calculi, Bisimulation, Operational Congruences, Term Rewriting, Labelled Transition Systems.

Contents

1 Introduction 2

2 Ground term rewriting 6

3 Term rewriting with left-linear rules 10

4 Term rewriting with left-linear rules, parallel and blocking 17

5 Conclusion 28

A Proofs for Section 2 31

B Proofs for Section 3 32

Preprint submitted to Elsevier Preprint *17 December 1999*

C Proofs for Section 4 37

C.1 Dissection Lemmas 38

C.2 Forwards Lemmas 40

C.3 Backwards Lemmas 48

References 50

1 Introduction

The dynamic behaviour of many calculi can be defined most clearly by a *reduction semantics*, comprising a set of rewrite rules, a set of reduction contexts in which they may be applied, and a structural congruence. These define the atomic internal reduction steps of terms. To work with a calculus, however, a compositional understanding of the behaviour of arbitrary subterms, as given by some operational congruence relation, is usually required. The literature contains investigations of such congruences for a large number of particular calculi. They are often given tractable definitions or characterisations via *labelled transition relations*, capturing the potential external interactions between subterms and their environments. Defining labelled transitions that give rise to satisfactory operational congruences generally requires some mix of calculus-specific ingenuity and routine work.

In this paper the problem is addressed for arbitrary calculi of certain simple forms. We give general definitions of labelled transitions that depend only on a reduction semantics, without requiring any additional observations to be prescribed. We first consider term rewriting, with ground or left-linear rules, over an arbitrary signature but without a structural congruence. We then consider calculi with arbitrary signatures containing symbols 0 and $|$, a structural congruence consisting of associativity, commutativity and unit, left-linear rules, and non-trivial sets of reduction contexts. This suffices, for example, to express CCS-style synchronisation. It is essentially the same as the class of Action Calculi in which all controls have arity $0 \to 0$ and take some number of arguments of arity $0 \to 0$. In each case we define labelled transitions, prove that bisimulation is a congruence and give some comparison results.

Background: From reductions to labelled transitions to reductions... Definitions of the dynamics (or small-step operational semantics) of lambda calculi and sequential programming languages have commonly been given as reduction relations. The λ-calculus has the rewrite rule $(\lambda x.M)N \longrightarrow M[N/x]$ of β reduction, which can be applied in any context. For programming languages, some control of the order of evaluation is usually required. This has been done with abstract machines, in which the states, and reductions between them, are ad-hoc mathematical objects. More elegantly, one can give definitions in the structural operational semantics (SOS) style of Plotkin [33]; here the states are terms of the language (sometimes augmented by e.g. a store), the reductions are given by a syntax-directed inductive definition. Explicit reformulations using rewrite rules and reduction contexts were first given by Felleisen and Friedman [15]. (We here neglect semantics in the big-step/evaluation/natural style.)

In contrast, until recently, definitions of operational semantics for process calculi have been primarily given as labelled transition relations. The central reason for the difference is not mathematical, but that lambda and process terms have had quite different intended interpretations. The standard interpretation of lambda terms and functional programs is that they specify computations which may either not terminate, or terminate with some result that cannot reduce further. Confluence properties ensure that such result terms are unique if they exist; they can implicitly be examined, either up to equality or up to a coarser notion. The theory of processes, however, inherits from automata theory the view that process terms may both reduce internally and interact with their environments; labelled transitions allow these interactions to be expressed. Reductions may create or destroy potential interactions. Termination of processes is usually not a central concept, and the structure of terms, even of terms that cannot reduce, is not considered examinable.

An additional, more technical, reason is that definitions of the reductions for a process calculus require either auxiliary labelled transition relations or a non-trivial structural congruence. For example, consider the CCS fragment below.

$$P ::= 0 \;\Big|\; \alpha.P \;\Big|\; \bar{\alpha}.P \;\Big|\; P \,|\, P \qquad \alpha \in \mathcal{A}$$

Its standard semantics has reductions $P \longrightarrow Q$ but also labelled transitions $P \xrightarrow{\alpha} Q$ and $P \xrightarrow{\bar{\alpha}} Q$. These represent the potentials that P has for synchronising on α. They can be defined by an SOS

$$\textsc{Out}\ \frac{}{\bar{\alpha}.P \xrightarrow{\bar{\alpha}} P} \qquad\qquad \textsc{In}\ \frac{}{\alpha.P \xrightarrow{\alpha} P}$$

$$\textsc{Com}\ \frac{P \xrightarrow{\bar{\alpha}} P' \quad Q \xrightarrow{\alpha} Q'}{P \,|\, Q \longrightarrow P' \,|\, Q'} \qquad \textsc{Com}'\ \frac{P \xrightarrow{\alpha} P' \quad Q \xrightarrow{\bar{\alpha}} Q'}{P \,|\, Q \longrightarrow P' \,|\, Q'}$$

$$\textsc{Par}\ \frac{P \xrightarrow{\mu} Q}{P \,|\, R \xrightarrow{\mu} Q \,|\, R} \qquad\qquad \textsc{Par}'\ \frac{P \xrightarrow{\mu} Q}{R \,|\, P \xrightarrow{\mu} R \,|\, Q}$$

where $\xrightarrow{\mu}$ is either $\longrightarrow$, $\xrightarrow{\alpha}$ or $\xrightarrow{\bar{\alpha}}$. It has been noted by Berry and Boudol [7], following work of Banâtre and Le Métayer [5] on the Γ language, that semantic definitions of process calculi could be simplified by working modulo an equivalence that allows the parts of a redex to be brought syntactically adjacent. Their presentation is in terms of Chemical Abstract Machines; in a slight variation we give a reduction semantics for the CCS fragment above. It consists of the rewrite rule $\bar{\alpha}.P \,|\, \alpha.Q \longrightarrow P \,|\, Q$, the set of reduction contexts given by

$$C ::= \_ \;\Big|\; C \,|\, P \;\Big|\; P \,|\, C$$

and the structural congruence $\equiv$ defined to be the least congruence satisfying $P \equiv P \,|\, 0$, $P \,|\, Q \equiv Q \,|\, P$ and $P \,|(Q \,|\, R) \equiv (P \,|\, Q) \,|\, R$. Modulo use of $\equiv$ on the right, this gives exactly the same reductions as before. For this toy calculus the two definitions are of similar complexity. For the π-calculus ([27], building on [14]), however, Milner has given a reduction semantics that is much simpler than the rather delicate SOS definitions of π labelled transition systems [28]. Following this, more recent name passing process calculi have often been defined by a reduction semantics in some form, e.g. the HOπ [35], ρ [32], Join [17], Blue [9], Spi [1], dpi [39], Dπ [34] and Ambient [10] Calculi.

Turning to operational congruences, for confluent calculi the definition of an appropriate operational congruence is relatively straightforward, even in the (usual) case where the dynamics are expressed as a reduction relation. For example, for a simple eager functional programming language, with a base type Int of integers, terminated states of programs of type Int are clearly observable up to equality. These basic observations can be used to define a Morris-style operational congruence. Several authors have considered tractable characterisations of these congruences in terms of bisimulation – see e.g. [25,2,21] and the references therein, and [22] for related work on an object calculus.

For non-confluent calculi the situation is more problematic – process calculi having labelled transition semantics have been equipped with a plethora of different operational equivalences, whereas rather few styles of definition have been proposed for those having reduction semantics. In the labelled transition case there are many more-or-less plausible notions of observation, differing e.g. in their treatment of linear/branching time, of internal reductions, of termination and divergence, etc. Some of the space is illustrated in the surveys of van Glabbeek [19,20]. The difficulty here is to select a notion that is appropriate for a particular application; one attempt is in [36]. In the reduction case we have the converse problem – a reduction relation does not of itself seem to support any notion of observation that gives rise to a satisfactory operational congruence. This was explicitly addressed for CCS and π-calculi by Milner and Sangiorgi in [30,35], where barbed bisimulation equivalences are defined in terms of reductions and observations of *barbs*. These are vestigial labelled transitions, similar to the distinguished observable transitions in the *tests* of De Nicola and Hennessy [12]. The expressive power of their calculi suffices to recover early labelled transition bisimulations as the induced congruences. Related work of Honda and Yoshida [24] uses *insensitivity* as the basic observable; that of Montanari and Sassone [31] takes the usual CCS labelled transitions but by requiring context-closure at every step of a bisimulation gives the coarsest notion of weak bisimulation that is simultaneously a congruence. Rensink [40] studies bisimulation directly on open terms.

...to labelled transitions Summarizing, definitions of operational congruences, for calculi having reduction semantics, have generally been based either on observation of terminated states, in the confluent case, or on observation of some barbs, where a natural definition of these exists. In either case, characterisations of the congruences in terms of labelled transitions, involving as little quantification over contexts as possible, are desirable. Moreover, some reasonable calculi may not have a natural definition of barb that induces an appropriate congruence.

In this paper we show that labelled transitions that give rise to bisimulation congruences can be defined purely from the reduction semantics of a calculus, without prescribing any additional observations. We consider only simple classes of reduction semantics, not involving name or variable binding, but hope that these will be a first step towards a generally applicable theory. As a test of the definitions we show that they recover the usual bisimulation on the CCS fragment above. We also discuss term rewriting and a fragment of the Ambient calculus of Cardelli and Gordon. To directly express the semantics of more interesting calculi requires a richer framework. One must deal with binding, with rewrite rules involving term or name substitutions, with a structural congruence that allows scope mobility, and with more delicate sets of reduction contexts. The *Action Calculi* of Milner [29] are a candidate framework that allows several of the calculi mentioned above to be defined cleanly; this work can be seen as a step towards understanding operational congruences for arbitrary action calculi. Bisimulation for a particular action calculus, representing a π-calculus, has been studied by Mifsud [26]. More generally (in work that is yet to be published), Jensen has considered a form of graph rewriting that idealizes action calculi and Leifer has studied classes of Action Calculi obeying certain arity restrictions. The approaches adopted in these and in the current work are closely related.

Labelled transitions intuitively capture the possible interactions between a term and a surrounding context. The central idea of this work is to make this intuition explicit – the labels of transitions from a term s will be contexts that, when applied to s, create an occurrence of a rewrite rule. In the next three sections we develop the theory for ground term rewriting, then for left-linear term rewriting, and then with the addition of an ACI (associativity, commutativity and identity) structural congruence and reduction contexts. Section 5 contains some concluding remarks. Most proofs are banished to the appendices or omitted; details can be found in the technical report [37]. An extended abstract appeared in [38].

2 Ground term rewriting

In this section we consider one of the simplest possible classes of reduction semantics, that of ground term rewriting. The definitions and proofs are here rather straightforward, but provide a guide to those in the following two sections.

Reductions We take essentially standard definitions of rewrite systems (see e.g. [4] for an introduction) but for convenience in later sections work with contexts and context composition rather than open terms and substitution. We fix a *signature* consisting of a (possibly infinite) set Σ of function symbols, ranged over by σ, and an arity function $|\_|$ from Σ to $\mathbb{N}$. We say an n-hole context over the signature, with holes $\_{}_1, \ldots, \_{}_n$, is *linear* if it has exactly one occurrence of each of the n holes. In this section a, b, l, r, s, t range over terms, A, B, C, D, F, H range over linear unary contexts and E ranges over linear binary contexts. Context composition and application of contexts to (tuples of) terms are written $A \cdot B$ and $A \cdot s$, the identity context as $\_$ and tupling with $+$. We take a (possibly infinite) set $\mathcal{R}$ of *rewrite rules*, each consisting of a pair $\langle l, r\rangle$ of terms. The *reduction relation* between terms over Σ is then

$$s \longrightarrow t \overset{def}{\Leftrightarrow} \exists \langle l, r\rangle \in \mathcal{R}, C \,.\; s = C \cdot l \wedge C \cdot r = t$$

Labelled Transitions The transitions of a term s will be labelled by linear unary contexts. Transitions $s \xrightarrow{\_} t$ labelled by the identity context are simply reductions (analogous to τ-transitions). Transitions $s \xrightarrow{F} t$ for $F \neq \_$ indicate that applying F to s creates an instance of a rewrite rule, with target instance t. For example, given a signature with constants β and δ, a unary γ, and the rule

$$\gamma(\beta) \longrightarrow \delta$$

we will have labelled transitions

$$C \cdot \gamma(\beta) \xrightarrow{\_} C \cdot \delta$$

for all C and also

$$\beta \xrightarrow{\gamma(\_)} \delta$$

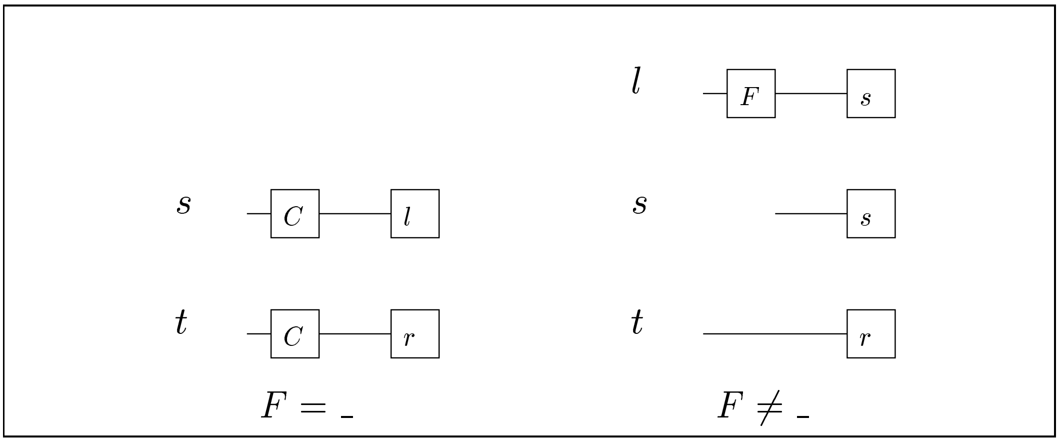

Fig. 1. Contextual Labelled Transitions $s \xrightarrow{F} t$ for Ground Term Rewriting.

but not

$$\beta \xrightarrow{C \cdot \gamma(\_)} C \cdot \delta$$

for $C \neq \_$. The *labels* are $\{\, F \mid \exists \langle l, r \rangle \in \mathcal{R}, s \,.\; F \cdot s = l \,\}$ and the *contextual labelled transition relations* $\xrightarrow{F}$ are defined by the clauses below, illustrated in Figure 1.

- $s \xrightarrow{\_} t \overset{def}{\Leftrightarrow} s \longrightarrow t$
- $s \xrightarrow{F} t \overset{def}{\Leftrightarrow} \exists \langle l, r \rangle \in \mathcal{R} \,.\; F \cdot s = l \wedge r = t \qquad$ for $F \neq \_$

Bisimulation Congruence Let $\sim$ be strong bisimulation with respect to these transitions, i.e. the largest binary relation over terms such that for any $s \sim s'$

- $s \xrightarrow{F} t \implies \exists t' \,.\; s' \xrightarrow{F} t' \wedge t \sim t'$
- $s' \xrightarrow{F} t' \implies \exists t \,.\; s \xrightarrow{F} t \wedge t \sim t'$

The congruence proof for $\sim$ is straightforward. It is given in some detail as a guide to the more intricate corresponding proofs in the following two sections, which have the same structure. Three lemmas (2–4) show how contexts in labels and in the sources of transitions interrelate; they are proved by case analysis using a dissection lemma which is standard folklore.

Lemma 1 (Dissection) *If $A \cdot a = B \cdot b$ then one of the following cases holds.*

(1) *(b is in a) There exists D such that $a = D \cdot b$ and $A \cdot D = B$.*
(2) *(a is properly in b) There exists D with $D \neq \_$ such that $D \cdot a = b$ and $A = B \cdot D$.*
(3) *(a and b are disjoint) There exists E such that $A = E \cdot (\_ + b)$ and $B = E \cdot (a + \_)$.*

Lemma 2 (Forwards-1) *If $A \cdot s \xrightarrow{\_} t$ then one of the following holds:*

(1) There exists some H such that $t = H \cdot s$ and for any $\hat{s}$ we have $A \cdot \hat{s} \xrightarrow{\_} H \cdot \hat{s}$.
(2) There exists some $\hat{t}$, A_1 and A_2 such that $A = A_1 \cdot A_2$, $s \xrightarrow{A_2} \hat{t}$ and $t = A_1 \cdot \hat{t}$.

Proof By the definition of reduction

$$\exists \langle l, r \rangle \in \mathcal{R}, C\,.\;\; A \cdot s = C \cdot l \wedge C \cdot r = t$$

Applying the dissection lemma (Lemma 1) to $A \cdot s = C \cdot l$ gives the following cases.

(1) (l is in s) There exists B such that $s = B \cdot l$ and $A \cdot B = C$. Taking $\hat{t} = B \cdot r$, $A_1 = A$ and $A_2 = \_$ the second clause holds.
(2) (s is properly in l) There exists B with $B \neq \_$ such that $B \cdot s = l$ and $A = C \cdot B$. Taking $\hat{t} = r$, $A_1 = C$ and $A_2 = B$ the second clause holds.
(3) (s and l are disjoint) There exists E such that $A = E \cdot (\_ + l)$ and $C = E \cdot (s + \_)$. Taking $H = E \cdot (\_ + r)$ the first clause holds.

$\square$

Lemma 3 (Forwards-2) *If $A \cdot s \xrightarrow{F} t$ and $F \neq \_$ then $s \xrightarrow{F \cdot A} t$.*

Proof By the definition of labelled transitions $\exists \langle l, r \rangle \in \mathcal{R}\,.\;\; F \cdot A \cdot s = l \wedge r = t$. Clearly $F \cdot A$ is linear and $F \cdot A \neq \_$ so $s \xrightarrow{F \cdot A} t$. $\square$

Lemma 4 (Backwards) *If $s \xrightarrow{F \cdot A} t$ then $A \cdot s \xrightarrow{F} t$.*

Proof If $F \cdot A = \_$ then $F = A = \_$ so the conclusion is immediate, otherwise by the definition of transitions $\exists \langle l, r \rangle \in \mathcal{R}\,.\;\; F \cdot A \cdot s = l \wedge r = t$. One then has $A \cdot s \xrightarrow{F} t$ by the definition of transitions, by cases for $F \neq \_$ and $F = \_$. $\square$

Proposition 5 *$\sim$ is a congruence.*

Proof We show

$$\mathcal{S} \stackrel{def}{=} \{\, A \cdot s, A \cdot s' \mid s \sim s' \wedge A : 1 \to 1 \text{ linear} \,\}$$

is a bisimulation.

(1) Suppose $A \cdot s \xrightarrow{\_} t$.
By Lemma 2 one of the following holds:
(a) There exists some H such that $t = H \cdot s$ and for any $\hat{s}$ we have $A \cdot \hat{s} \xrightarrow{\_} H \cdot \hat{s}$.
Instantiating, $A \cdot s' \xrightarrow{\_} H \cdot s'$, and clearly $H \cdot s \;\mathcal{S}\; H \cdot s'$.
(b) There exists some $\hat{t}$, A_1 and A_2 such that $A = A_1 \cdot A_2$, $s \xrightarrow{A_2} \hat{t}$ and $t = A_1 \cdot \hat{t}$.

By $s \sim s'$ there exists $\hat{t}'$ such that $s' \xrightarrow{A_2} \hat{t}' \sim \hat{t}$.
By Lemma 4 $A_2 \cdot s' \xrightarrow{-} \hat{t}'$.
By the definition of reduction $A_1 \cdot A_2 \cdot s' \xrightarrow{-} A_1 \cdot \hat{t}'$, and clearly $A_1 \cdot \hat{t} \; \mathcal{S} \; A_1 \cdot \hat{t}'$.

(2) Suppose $A \cdot s \xrightarrow{F} t$ for $F \neq \_$.
By Lemma 3 $s \xrightarrow{F \cdot A} t$.
By $s \sim s'$ there exists t' such that $s' \xrightarrow{F \cdot A} t' \sim t$.
By Lemma 4 $A \cdot s' \xrightarrow{F} t'$, and clearly $t \; \mathcal{S} \; t'$.

□

Remark An alternative approach would be to take transitions

- $s \xrightarrow{F}_{\text{alt}} t \overset{def}{\Leftrightarrow} F \cdot s \longrightarrow t$

for unary linear contexts F. Note that these are defined using only the reduction relation, whereas the definition above involved the reduction rules. Let $\sim_{\text{alt}}$ be strong bisimulation with respect to these transitions. One can show that $\sim_{\text{alt}}$ is a congruence and moreover is unaffected by cutting down the label set to that considered above. In general $\sim_{\text{alt}}$ is strictly coarser than $\sim$. For an example of the non-inclusion, if the signature consists of constants α, β and a unary symbol γ with reduction rules $\alpha \longrightarrow \alpha$, $\beta \longrightarrow \beta$ and $\gamma(\beta) \longrightarrow \beta$, then $\alpha \not\sim \beta$ whereas $\alpha \sim_{\text{alt}} \beta$. The details can be found in Appendix A. This insensitivity to the possible interactions of terms that have internal transitions suggests that the analogue of $\sim_{\text{alt}}$, in more expressive settings, is unlikely to coincide with standard bisimulations for particular calculi. Indeed, one can show that applying the alternative definition to the fragment of CCS

$$P ::= 0 \;\Big|\; \alpha \;\Big|\; \bar{\alpha} \;\Big|\; P \,|\, P \qquad \alpha \in \mathcal{A}$$

(with its usual reduction relation as defined in Section 1) gives an equivalence that identifies $\alpha \,|\, \bar{\alpha}$ with $\beta \,|\, \bar{\beta}$ for $\alpha, \beta \in \mathcal{A}$; these are not identified in any reasonable operational congruence.

Remark In the proofs of Lemmas 2–4 the labelled transition exhibited for the conclusion involves the same rewrite rule as the transition in the premise. One could therefore take the finer transitions

- $s \xrightarrow{-} t \overset{def}{\Leftrightarrow} s \longrightarrow t$
- $s \xrightarrow{F}_{\langle l,r \rangle} t \overset{def}{\Leftrightarrow} \langle l, r \rangle \in \mathcal{R} \wedge F \cdot s = l \wedge r = t \qquad$ for $F \neq \_$

annotated by the rewrite rule involved, and still have a congruence result. In some cases this gives a finer bisimulation relation (c.f. the arithmetic example in Section 3). There are intermediate definitions – in fact any partition of the rule set $\mathcal{R}$ gives rise to a bisimulation that is a congruence relation, taking labelled transitions annotated by the equivalence class of the rule involved.

3 Term rewriting with left-linear rules

In this section the definitions are generalised to left-linear term rewriting, as a second step towards a framework expressive enough for simple process calculi.

Notation In the next two sections we must consider more complex dissections of contexts and terms. It is convenient to treat contexts and terms uniformly, working with n-tuples of m-hole contexts for $m, n \geq 0$. Concretely, we work in the category $\mathbb{C}_\Sigma$ that has the natural numbers as objects and arrows

$$\frac{i \in 1..m}{\langle \_{i} \rangle_m : m \to 1} \qquad \frac{\langle a_1 \rangle_m : m \to 1 \;\; \cdots \;\; \langle a_n \rangle_m : m \to 1}{\langle a_1, \ldots, a_n \rangle_m : m \to n} \qquad \frac{\langle a_1, \ldots, a_{|\sigma|} \rangle_m : m \to |\sigma|}{\langle \sigma(a_1, \ldots, a_{|\sigma|}) \rangle_m : m \to 1}$$

The identity on m is $\mathbf{id}_m \stackrel{\mathit{def}}{=} \langle \_{1}, \ldots, \_{m} \rangle_m$, composition is substitution, with $\langle a_1, \ldots, a_n \rangle_m \cdot \langle b_1, \ldots, b_m \rangle_l = \langle a_1[b_1/\_{1}, \ldots, b_m/\_{m}], \ldots, a_n[b_1/\_{1}, \ldots, b_m/\_{m}] \rangle_l$. $\mathbb{C}_\Sigma$ has strictly associative binary products, written with $+$. If $a : m \to k$ and $b : m \to l$ we write $a \oplus b$ for $(a + b) \cdot \langle \_{1}, \ldots, \_{m}, \_{1}, \ldots, \_{m} \rangle_m : m \to k + l$. Angle brackets and domain subscripts will often be elided. We let $a, b, e, q, r, s, t, u, v$ range over $0 \to m$ arrows, i.e. m-tuples of terms, and $A, B, \ldots$ range over $m \to 1$ arrows, i.e. m-hole contexts. Say an arrow is a *permutation* if it is of the form $\langle \_{\Pi(1)}, \ldots, \_{\Pi(m)} \rangle_m$ where Π is a permutation of the set $\{1, \ldots, m\}$. A family of arrows $\pi_i : m \to m_i$ for $i \in 1..k$ where $m_1 + \ldots + m_k = m$ is a *partition* if $\pi_1 \oplus \ldots \oplus \pi_m$ is a permutation. We write $\mathbf{perm}_{m,n}$ for the permutation $\langle \_{n+1}, \ldots, \_{n+m}, \_{1}, \ldots, \_{n} \rangle_{m+n} : n + m \to m + n$. Say an arrow $\langle a_1, \ldots, a_n \rangle_m$ is *linear* if it contains exactly one occurrence of each $\_{1}, \ldots, \_{m}$ and *affine* if it contains at most one occurrence of each. We sometimes abuse notation in examples, writing $\_, \_{1}, \_{2}, \ldots$ instead of $\_{1}, \_{2}, \_{3}, \ldots$.

Remark Many slight variations of $\mathbb{C}_\Sigma$ are possible. We have chosen to take the objects to be natural numbers, instead of finite sets of variables, to give a lighter notation for labels. The concrete syntax is chosen so that arrows from 0 to 1 are exactly the standard terms over Σ, modulo elision of the angle brackets and subscript 0.

Reductions The usual notion of left-linear term rewriting is now expressible as follows. We take a (possibly infinite) set $\mathcal{R}$ of *rewrite rules*, each consisting of a triple $\langle n, L, R \rangle$ where $n \geq 0$, $L : n \to 1$ is linear and $R : n \to 1$. The *reduction relation* over $\{ s \mid s : 0 \to 1 \}$ is then defined by

$$s \longrightarrow t \stackrel{\mathit{def}}{\Leftrightarrow} \exists \langle m, L, R \rangle \in \mathcal{R},\; C : 1 \to 1 \text{ linear},\; u : 0 \to m \,.\; s = C \cdot L \cdot u \wedge C \cdot R \cdot u = t$$

Labelled Transitions The labelled transitions of a term $s:0\to 1$ will again be of two forms, $s\xrightarrow{\_}t$, for internal reductions, and $s\xrightarrow{F}T$ where $F\neq\_$ is a context that, together with part of s, makes up the left hand side of a rewrite rule. For example, given the rule

$$\delta(\gamma(\_))\longrightarrow\epsilon(\_)$$

we will have labelled transitions

$$\gamma(s)\xrightarrow{\delta(\_)}\epsilon(s)$$

for all terms $s:0\to 1$. Labelled transitions in which the label contributes the whole of the left hand side of a rule would be redundant (they are not required in the congruence proof), so the definition will exclude e.g. $s\xrightarrow{\delta(\gamma(\_))}\epsilon(s)$. Now consider the rule

$$\sigma(\alpha,\gamma(\_))\longrightarrow\epsilon(\_)$$

As before there will be labelled transitions

$$\gamma(s)\xrightarrow{\sigma(\alpha,\_)}\epsilon(s)$$

for all s. In addition, one can construct instances of the rule by placing the term α in contexts $\sigma(\_,\gamma(t))$, suggesting labelled transitions $\alpha\xrightarrow{\sigma(\_,\gamma(t))}\epsilon(t)$ for any t. Instead, to keep the label sets small, and to capture the uniformity in t, we allow both labels and targets of transitions to be parametric in uninstantiated arguments of the rewrite rule. In this case the definition will give

$$\alpha\xrightarrow{\sigma(\_,\gamma(\_1))}\epsilon(\_1)$$

In general, then, the *contextual labelled transitions* are of the form $s\xrightarrow{F}T$, for $s:0\to 1$, $F:1+n\to 1$ and $T:n\to 1$. The first argument of F is the hole in which s can be placed to create an instance of a rule L; the other n arguments are parameters of L that are not thereby instantiated. The transitions are defined as follows.

- $s\xrightarrow{\_}T \overset{def}{\Leftrightarrow} s\longrightarrow T$.
- $s\xrightarrow{F}T$, for $F:1+n\to 1$ linear and not the identity, iff there exist

$\langle m,L,R\rangle\in\mathcal{R}$ with $m\geq n$
$\pi:m\to m$ a permutation
$L_1:(m-n)\to 1$ linear and not the identity
$u:0\to(m-n)$

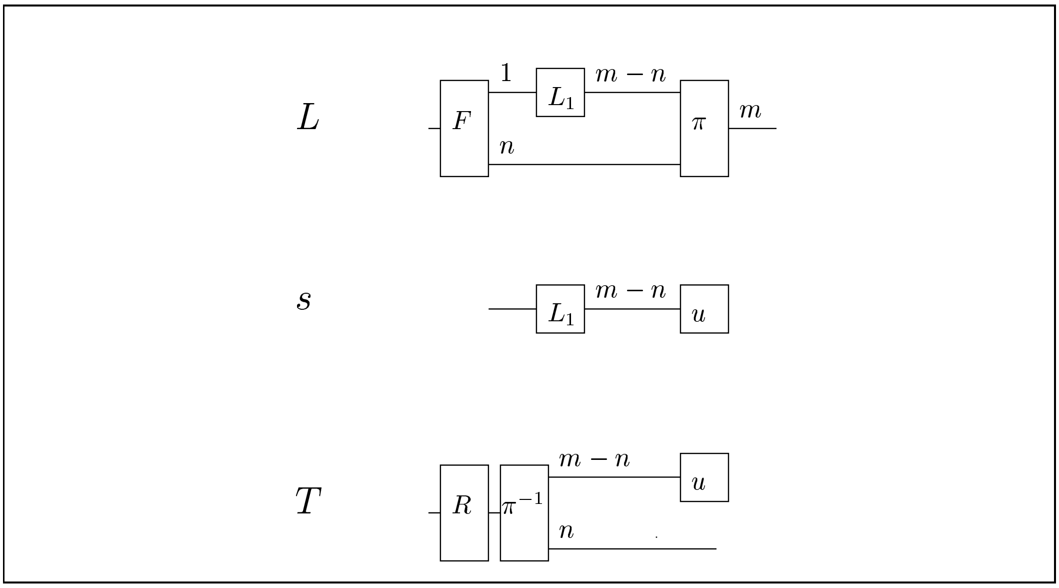

Fig. 2. Contextual Labelled Transitions for Left-Linear Term Rewriting. Boxes with m input wires (on their right) and n output wires (on their left) represent n-tuples of m-hole contexts. Wires are ordered from top to bottom.

such that

$$\begin{aligned} L &= F \cdot (L_1 + \mathbf{id}_n) \cdot \pi \\ s &= L_1 \cdot u \\ T &= R \cdot \pi^{-1} \cdot (u + \mathbf{id}_n) \end{aligned}$$

The definition is illustrated in Figure 2. The restriction to $L_1 \neq \mathbf{id}_1$ excludes transitions where the label contributes the whole of L. The permutation π is required so that the parameters of L can be divided into the instantiated and uninstantiated. For example the rule

$$\rho(\delta(\_1), \gamma(\_2), \beta) \longrightarrow \sigma(\_1, \_2)$$

will give rise to transitions

$$\begin{array}{llll} \delta(s) \xrightarrow{\rho(\_, \gamma(\_1), \beta)} \sigma(s, \_1) & & \beta \xrightarrow{\rho(\delta(\_1), \gamma(\_2), \_)} \sigma(\_1, \_2) \\ \gamma(s) \xrightarrow{\rho(\delta(\_1), \_, \beta)} \sigma(\_1, s) & & \beta \xrightarrow{\rho(\delta(\_2), \gamma(\_1), \_)} \sigma(\_2, \_1) \end{array}$$

(The last is redundant; it could be excluded by requiring π to be a monotone partition of m into $m-n$ and n.)

Bisimulation Congruence A binary relation $\mathcal{S}$ over terms $\{\, a \mid a : 0 \to 1 \,\}$ is lifted to a relation over $\{\, A \mid A : n \to 1 \,\}$ by $A \; [\mathcal{S}] \; A' \overset{def}{\Leftrightarrow} \forall b : 0 \to n \,.\; A \cdot b \; \mathcal{S} \; A' \cdot b$. Say $\mathcal{S}$ is a bisimulation if for any $s \; \mathcal{S} \; s'$

- $s \xrightarrow{F} T \implies \exists T' .\; s' \xrightarrow{F} T' \wedge T \; [\mathcal{S}] \; T'$
- $s' \xrightarrow{F} T' \implies \exists T .\; s \xrightarrow{F} T \wedge T \; [\mathcal{S}] \; T'$

and write $\sim$ for the largest such. As before the congruence proof requires a simple dissection lemma and three lemmas relating contexts in sources and labels. Their proofs can be found in Appendix B.

Lemma 6 (Dissection) *If $A \cdot a = B \cdot b$, for $m \geq 0$, $A : 1 \to 1$ and $B : m \to 1$ linear, $a : 0 \to 1$ and $b : 0 \to m$ then one of the following holds.*

(1) (a is not in any component of b) There exist

$$\begin{array}{l} m_1 \textit{ and } m_2 \textit{ such that } m_1 + m_2 = m \\ \pi_i : m \to m_i \textit{ for } i \in \{1,2\} \textit{ a partition} \\ C : 1 + m_2 \to 1 \textit{ linear} \\ D : m_1 \to 1 \textit{ linear and not the identity} \end{array}$$

such that

$$\begin{aligned} A &= C \cdot (\mathbf{id}_1 + \pi_2 \cdot b) \\ a &= D \cdot \pi_1 \cdot b \\ B &= C \cdot (D + \mathbf{id}_{m_2}) \cdot (\pi_1 \oplus \pi_2) \end{aligned}$$

i.e. there are m_1 components of b in a and m_2 in A.

(2) (a is in a component of b) $m \geq 1$ and there exist

$$\begin{array}{l} \pi_1 : m \to 1 \textit{ and } \pi_2 : m \to (m-1) \textit{ a partition} \\ E : 1 \to 1 \textit{ linear} \end{array}$$

such that

$$\begin{aligned} A &= B \cdot (\pi_1 \oplus \pi_2)^{-1} \cdot (E + \pi_2 \cdot b) \\ E \cdot a &= \pi_1 \cdot b \end{aligned}$$

Lemma 7 (Forwards-1) *If $A \cdot s \xrightarrow{-} t$ and $A : 1 \to 1$ linear then one of the following holds.*

(1) There exists some $H : 1 \to 1$ such that $t = H \cdot s$ and for all $\hat{s} : 0 \to 1$ we have $A \cdot \hat{s} \xrightarrow{-} H \cdot \hat{s}$.
(2) There exist $k \geq 0$, $F : 1 + k \to 1$ linear, $T : k \to 1$, $D : 1 \to 1$ linear and $v : 0 \to k$, such that $s \xrightarrow{F} T$, $A = D \cdot F \cdot (\mathbf{id}_1 + v)$ and $t = D \cdot T \cdot v$.

Lemma 8 (Forwards-2) *If $A \cdot s \xrightarrow{F} T$ for $A : 1 \to 1$ linear, $F : 1 + n \to 1$ and $F \neq \mathbf{id}_1$ then one of the following holds.*

(1) There exists $H : 1 + n \to 1$ such that $T = H \cdot (s + \mathbf{id}_n)$ and for all $\hat{s} : 0 \to 1$ we have $A \cdot \hat{s} \xrightarrow{F} H \cdot (\hat{s} + \mathbf{id}_n)$.
(2) There exist $p \geq 0$, $E : 1 + p \to 1$ linear, $\hat{T} : p + n \to 1$ and $v : 0 \to p$, such that $s \xrightarrow{F \cdot (E + \mathbf{id}_n)} \hat{T}$, $T = \hat{T} \cdot (v + \mathbf{id}_n)$ and $A = E \cdot (\mathbf{id}_1 + v)$.

Lemma 9 (Backwards) *If* $s \xrightarrow{C\cdot(E+\mathbf{id}_n)} T$ *for* $E : 1 + p \to 1$ *linear and* $C : 1 + n \to 1$ *linear then for all* $v : 0 \to p$ *we have* $E\cdot(s + v) \xrightarrow{C} T\cdot(v + \mathbf{id}_n)$.

Theorem 10 $\sim$ *is a congruence.*

Proof We show $\mathcal{S}^*$, where

$$\mathcal{S} \stackrel{def}{=} \{\, A\cdot s, A\cdot s' \mid s \sim s' \wedge A : 1 \to 1 \text{ linear}\,\}$$

is a bisimulation. First note that for any (possibly non-linear) $A : 1 \to 1$ and $s \sim s'$ we have $A\cdot s\ \mathcal{S}^*\ A\cdot s'$. To see this, take $n \geq 0$ and $\hat{A} : n \to 1$ linear such that $A = \hat{A}\cdot\langle \_{1}, \ldots, \_{1}\rangle_1$. Let

$$\begin{aligned}
A_1 &\stackrel{def}{=} \hat{A}\cdot\langle _{1}, s, s, \ldots, s\rangle_1 \\
A_2 &\stackrel{def}{=} \hat{A}\cdot\langle s', _{1}, s, \ldots, s\rangle_1 \\
&\ldots \\
A_n &\stackrel{def}{=} \hat{A}\cdot\langle s', s', s', \ldots, _{1}\rangle_1
\end{aligned}$$

Each A_i is linear, so $A_i\cdot s\ \mathcal{S}\ A_i\cdot s'$. Moreover $A_i\cdot s' = A_{i+1}\cdot s$ for $i \in 1..n-1$ so $A\cdot s = A_1\cdot s\ \mathcal{S}^n\ A_n\cdot s' = A\cdot s'$.

We now show that if $A : 1 \to 1$ linear, $s \sim s'$ and $A\cdot s \xrightarrow{F} T$ then there exists T' such that $A\cdot s' \xrightarrow{F} T'$ and $T\ [\mathcal{S}^*]\ T'$.

(1) Suppose $A\cdot s \xrightarrow{-} t$.
   By Lemma 7 one of the following holds:
   (a) There exists some $H : 1 \to 1$ such that $t = H\cdot s$ and for all $\hat{s} : 0 \to 1$ we have $A\cdot\hat{s} \xrightarrow{-} H\cdot\hat{s}$.
      Hence $A\cdot s' \xrightarrow{-} H\cdot s'$.
      Clearly $t = H\cdot s\ \mathcal{S}^*\ H\cdot s'$.
   (b) There exist $k \geq 0$, $F : 1 + k \to 1$ linear, $T : k \to 1$, $D : 1 \to 1$ linear and $v : 0 \to k$, such that $s \xrightarrow{F} T$, $A = D\cdot F\cdot(\mathbf{id}_1 + v)$ and $t = D\cdot T\cdot v$.
      By $s \sim s'$ there exists T' such that $s' \xrightarrow{F} T' \wedge T\ [\sim]\ T'$.
      By Lemma 9 $F\cdot(s' + v) \xrightarrow{-} T'\cdot v$.
      By the definition of reduction $A\cdot s' = D\cdot F\cdot(s' + v) \xrightarrow{-} D\cdot T'\cdot v$.
      Clearly $t = D\cdot T\cdot v\ \mathcal{S}^*\ D\cdot T'\cdot v$.

(2) Suppose $A\cdot s \xrightarrow{F} T$ for $F : 1 + n \to 1$ linear and $F \neq \mathbf{id}_1$.
   By Lemma 8 one of the following holds.
   (a) There exists $H : 1 + n \to 1$ such that $T = H\cdot(s + \mathbf{id}_n)$ and for all $\hat{s} : 0 \to 1$ we have $A\cdot\hat{s} \xrightarrow{F} H\cdot(\hat{s} + \mathbf{id}_n)$.
      Hence $A\cdot s' \xrightarrow{F} H\cdot(s' + \mathbf{id}_n)$
      Clearly $T = H\cdot(s + \mathbf{id}_n)\ [\mathcal{S}^*]\ H\cdot(s' + \mathbf{id}_n)$.

(b) There exist $p \geq 0$, $E : 1 + p \to 1$ linear, $\hat{T} : p + n \to 1$ and $v : 0 \to p$, such that $s \stackrel{F \cdot (E + \mathbf{id}_n)}{\longrightarrow} \hat{T}$, $T = \hat{T} \cdot (v + \mathbf{id}_n)$ and $A = E \cdot (\mathbf{id}_1 + v)$.

By $s \sim s'$ there exists $\hat{T}'$ such that $s' \stackrel{F \cdot (E + \mathbf{id}_n)}{\longrightarrow} \hat{T}' \wedge \hat{T} \; [\sim] \; \hat{T}'$.

By Lemma 9 $A \cdot s' = E \cdot (s' + v) \stackrel{F}{\longrightarrow} \hat{T}' \cdot (v + \mathbf{id}_n)$.

Clearly $T = \hat{T} \cdot (v + \mathbf{id}_n) \; [\mathcal{S}^*] \; \hat{T}' \cdot (v + \mathbf{id}_n)$.

Now if

$$A_1 \cdot s_1 \; \mathcal{S} \; A_1 \cdot s'_2 = A_2 \cdot s_2 \; \mathcal{S} \; \ldots \; \mathcal{S} \; A_{n-1} \cdot s'_n$$

for A_i linear and $s_i \sim s'_{i+1}$, for $i \in 1..n-1$, and $A_1 \cdot s_1 \stackrel{F}{\longrightarrow} T_1$ then by the above there exists T_n such that $A_{n-1} \cdot s'_n \stackrel{F}{\longrightarrow} T_n$ and $T_1 \; [\mathcal{S}^*]^n \; T_n$, so $T_1 \; [\mathcal{S}^*] \; T_n$.

□

Remark The definition of transitions above reduces to that of Section 2 if all rules are ground. For open rules, instead of allowing parametric labels, one could simply close up the rewrite rules under instantiation, by $\mathrm{Cl}(\mathcal{R}) = \{ \langle 0, L \cdot u, R \cdot u \rangle \mid \langle n, L, R \rangle \in \mathcal{R} \wedge u : 0 \to n \}$, and apply the earlier definition. In general this would give a strictly coarser congruence. For an example of the non-inclusion, take a signature consisting of a nullary α and a unary γ, with $\mathcal{R}$ consisting of the rules $\gamma(\_) \longrightarrow \gamma(\_)$ and $\gamma(\gamma(\alpha)) \longrightarrow \gamma(\gamma(\alpha))$. We have $\mathrm{Cl}(\mathcal{R}) = \{ \gamma^n \alpha, \gamma^n \alpha \mid n \geq 1 \}$. The transitions are

$$\begin{array}{rlrl} \gamma^n \alpha & \stackrel{\_}{\longrightarrow}_{\mathcal{R}} \gamma^n \alpha & \gamma^n \alpha & \stackrel{\_}{\longrightarrow}_{\mathrm{Cl}(\mathcal{R})} \gamma^n \alpha \\ \alpha & \stackrel{\gamma(\gamma(\_))}{\longrightarrow}_{\mathcal{R}} \gamma(\gamma(\alpha)) & \alpha & \stackrel{\gamma^n \_}{\longrightarrow}_{\mathrm{Cl}(\mathcal{R})} \gamma^n \alpha \\ \gamma(\alpha) & \stackrel{\gamma(\_)}{\longrightarrow}_{\mathcal{R}} \gamma(\gamma(\alpha)) & \gamma^m \alpha & \stackrel{\gamma^n \_}{\longrightarrow}_{\mathrm{Cl}(\mathcal{R})} \gamma^{m+n} \alpha \end{array}$$

for $m, n \geq 1$, so $\gamma(\alpha) \not\sim_{\mathcal{R}} \gamma(\gamma(\alpha))$ but $\gamma(\alpha) \sim_{\mathrm{Cl}(\mathcal{R})} \gamma(\gamma(\alpha))$. The proof of the following proposition can be found in Appendix B.

Proposition 11 *If $s \sim_{\mathcal{R}} s'$ then $s \sim_{\mathrm{Cl}(\mathcal{R})} s'$.*

Comparison Bisimulation as defined here is a congruence for arbitrary left-linear term rewriting systems. Much work on term rewriting deals with reduction relations that are confluent and terminating. In that setting terms have unique normal forms; the primary equivalence on terms is $\simeq$, where $s \simeq t$ if s and t have the same normal form. This is easily proved to be a congruence. In general, it is incomparable with $\sim$. To see one non-inclusion, note that $\sim$ is sensitive to atomic reduction steps; for the other that $\sim$ is not sensitive to equality of terms – for example, with only nullary symbols α, β, γ, and rewrite rule $\gamma \longrightarrow \beta$, we have $\alpha \sim \beta$ and $\beta \simeq \gamma$, whereas $\alpha \not\simeq \beta$ and $\beta \not\sim \gamma$. One might address the second non-inclusion by fiat, adding, for any value v, a unary test operator H_v and reduction rule $H_v(v) \longrightarrow v$. For the first, one might move to a weak bisimulation, abstracting from reduction steps. The simplest alternative is to take $\approx$ to be the largest relation $\mathcal{S}$ such that if $s \mathrel{\mathcal{S}} s'$ then

- $s \stackrel{-}{\longrightarrow} T \implies \exists T' .\ s' \stackrel{-}{\longrightarrow}^* T' \wedge T\ [\mathcal{S}]\ T'$
- $(s \stackrel{F}{\longrightarrow} T \wedge F \neq \_) \implies \exists T' .\ s' \stackrel{-}{\longrightarrow}^* \stackrel{F}{\longrightarrow} T' \wedge T\ [\mathcal{S}]\ T'$

and symmetric clauses.

Say the set $\mathcal{R}$ of rewrite rules is *right-affine* if the right hand side of each rule is affine. The following congruence result is proved in Appendix B; whether it holds without the restriction on $\mathcal{R}$ is left open.

Theorem 12 *If $\mathcal{R}$ is right-affine then $\approx$ is a congruence.*

Example – Arithmetic [1] Write $\approx'$ for the variant of $\approx$ defined using labelled transitions annotated by the rewrite rule involved, for transitions with non-identity labels. As before, the congruence proof for $\approx$ can easily be adapted to $\approx'$. For some rewrite systems $\approx'$ coincides with $\simeq$. Taking a signature Σ comprising nullary zero and unary succ and pred, and rewrite rules

$$\begin{array}{lr@{\ }l} (a) & \mathrm{pred}(\mathrm{succ}(\_{1})) \longrightarrow & \_{1} \\ (b) & \mathrm{pred}(\mathrm{zero}) \longrightarrow & \mathrm{zero} \end{array}$$

gives labelled transitions

$$\begin{array}{r} \mathrm{succ}(s) \stackrel{\mathrm{pred}(\_)}{\longrightarrow}_{(a)}\ s \\ \mathrm{zero} \stackrel{\mathrm{pred}(\_)}{\longrightarrow}_{(b)}\ \mathrm{zero} \end{array}$$

together with the reductions $\stackrel{-}{\longrightarrow}$. Here the normal forms are simply the naturals $\mathrm{succ}^n(\mathrm{zero})$ for $n \geq 0$; the relations $\approx'$ and $\simeq$ coincide with each other and with the standard equality on natural numbers. Note that in the non-annotated LTS every term has a weak transition $\stackrel{-}{\longrightarrow}^* \stackrel{\mathrm{pred}(\_)}{\longrightarrow}$ so the bisimulation $\approx$ will not be sufficiently discriminating.

In general, however, $\approx'$ and $\simeq$ still differ. For example, with unary γ, nullary α, and rules $\gamma(\alpha) \longrightarrow \alpha$ and $\gamma(\gamma(\alpha)) \longrightarrow \alpha$, we have $\alpha \not\approx' \gamma(\alpha)$ but all terms have normal form α. This may be a pathological rule set; one would like to have conditions excluding it under which $\approx'$ (or $\approx$) and $\simeq$ coincide.

Example – SKI Combinators Taking a signature Σ comprising nullary I, K, S and binary $\bullet$, and rewrite rules

$$\begin{array}{r@{\ }l} S \bullet \_{1} \bullet \_{2} \bullet \_{3} \longrightarrow & \_{1} \bullet \_{3} \bullet (\_{2} \bullet \_{3}) \\ K \bullet \_{1} \bullet \_{2} \longrightarrow & \langle \_{1} \rangle_2 \\ I \bullet \_{1} \longrightarrow & \_{1} \end{array}$$

[1] It should be noted that the example given in [37,38] contained errors.

gives labelled transitions

$$\begin{array}{rcl@{\qquad}rcl}
S & \xrightarrow{_ \bullet __1 \bullet __2 \bullet __3} & __1 \bullet __3 \bullet (__2 \bullet __3) & K & \xrightarrow{_ \bullet __1 \bullet __2} & \langle __1 \rangle_2 \\
S \bullet s & \xrightarrow{_ \bullet __1 \bullet __2} & s \bullet __2 \bullet (__1 \bullet __2) & K \bullet s & \xrightarrow{_ \bullet __1} & \langle s \rangle_1 \\
S \bullet s \bullet t & \xrightarrow{_ \bullet __1} & s \bullet __1 \bullet (t \bullet __1) & I & \xrightarrow{_ \bullet __1} & __1
\end{array}$$

together with some permutation instances of these and the reductions $\xrightarrow{\tau}$. The significance of $\sim$ and $\approx$ here is unclear. Note that the rules are not right-affine, so Theorem 12 does not guarantee that $\approx$ is a congruence – the question is open. It is quite intensional, being sensitive to the number of arguments that can be consumed immediately by a term. For example, $K \bullet (K \bullet s) \not\approx S \bullet (K \bullet (K \bullet s))$.

4 Term rewriting with left-linear rules, parallel and blocking

In this section we extend the setting to one sufficiently expressive to define the reduction relations of simple process calculi. We suppose the signature Σ includes binary and nullary symbols $|$ and 0, for parallel and nil, and take a structural congruence $\equiv$ generated by associativity, commutativity and identity axioms. Parallel will be written infix. The reduction rules $\mathcal{R}$ are as before. We now allow symbols to be *blocking*, i.e. to inhibit reduction in their arguments. For each $\sigma \in \Sigma$ we suppose given a set $\mathcal{B}(\sigma) \subseteq \{1, \ldots, |\sigma|\}$ defining the argument positions where reduction may take place. We require $\mathcal{B}(|) = \{1, 2\}$. The *reduction contexts* $\mathcal{C} \subseteq \{\, C \mid C : 1 \to 1 \text{ linear} \,\}$ are generated by

$$\mathbf{id}_1 \in \mathcal{C} \qquad \frac{i \in \mathcal{B}(\sigma) \quad \langle a \rangle_1 \in \mathcal{C}}{\langle \sigma(s_1, \ldots, s_{i-1}, a, s_{i+1}, \ldots, s_{|\sigma|}) \rangle_1 \in \mathcal{C}}$$

Formally, structural congruence is defined over all arrows of $\mathbb{C}_\Sigma$ as follows. It is a family of relations indexed by domain and codomain arities; the indexes will usually be elided. The first 3 rules impose the ACI properties of $|$; the others are congruence rules.

$$\frac{\langle a \rangle_m : m \to 1}{\langle a \rangle_m \equiv_{m,1} \langle a \mid 0 \rangle_m} \quad \frac{\langle a_i \rangle_m : m \to 1 \quad i \in \{1,2\}}{\langle a_1 \mid a_2 \rangle_m \equiv_{m,1} \langle a_2 \mid a_1 \rangle_m} \quad \frac{\langle a_i \rangle_m : m \to 1 \quad i \in \{1,2,3\}}{\langle a_1 \mid (a_2 \mid a_3) \rangle_m \equiv_{m,1} \langle (a_1 \mid a_2) \mid a_3 \rangle_m}$$

$$\frac{i \in 1..m}{\langle \_i \rangle_m \equiv_{m,1} \langle \_i \rangle_m} \qquad \frac{\langle a_i \rangle_m \equiv_{m,1} \langle b_i \rangle_m \quad i \in \{1..n\}}{\langle a_1..a_n \rangle_m \equiv_{m,n} \langle b_1..b_n \rangle_m}$$

$$\frac{f \equiv_{m,n} g}{g \equiv_{m,n} f} \qquad \frac{f \equiv_{m,n} g \quad g \equiv_{m,n} h}{f \equiv_{m,n} h} \qquad \frac{\langle a_1..a_{|\sigma|} \rangle_m \equiv_{m,|\sigma|} \langle b_1..b_{|\sigma|} \rangle_m}{\langle \sigma(a_1..a_{|\sigma|}) \rangle_m \equiv_{m,1} \langle \sigma(b_1..b_{|\sigma|}) \rangle_m}$$

Reductions The *reduction relation* over $\{\, s \mid s : 0 \to 1 \,\}$ is defined by $s \longrightarrow t$ iff

$$\exists \langle m, L, R \rangle \in \mathcal{R}, C \in \mathcal{C}, u : 0 \to m \,.\; s \equiv C \cdot L \cdot u \wedge C \cdot R \cdot u \equiv t$$

This class of calculi is essentially the same as the class of Action Calculi in which there is no substantive name binding, i.e. those in which all controls K have arity rules of the form

$$\frac{a_1 : 0 \to 0 \ \cdots \ a_r : 0 \to 0}{K(a_1, \ldots, a_r) : 0 \to 0}$$

(here the a_i are actions, not arrows from $\mathbb{C}_\Sigma$). It includes simple process calculi. For example, the fragment of CCS in Section 1 can be specified by taking a signature Σ_{CCS} consisting of unary $\alpha.$ and $\bar{\alpha}.$ for each $\alpha \in \mathcal{A}$, with 0 and $|$, and rewrite rules

$$\begin{aligned} \mathcal{R}_{\text{CCS}} &= \{ \langle 2,\ \alpha.\_1 \,|\, \bar{\alpha}.\_2,\ \_1 \,|\, \_2 \rangle \mid \alpha \in \mathcal{A} \} \\ \mathcal{B}_{\text{CCS}}(\alpha.) &= \mathcal{B}_{\text{CCS}}(\bar{\alpha}.) = \{\} \end{aligned}$$

Notation For a context $f : m \to n$ and $i \in 1..m$ say f is *shallow in argument* i if all occurrences of $\_i$ in f are not under any symbol except $|$. Say f is *deep in argument* i if any occurrence of $\_i$ in f is under some symbol not equal to $|$. Say f is *shallow* (*deep*) if it is shallow (deep) in all $i \in 1..m$. Say f is *i-separated* if there are no occurrences of any $\_j$ in parallel with an occurrence of $\_i$. Say f is *i-clean* if $\_i$ does not occur in parallel with any term, and f is *clean* if it is i-clean for all $i \in 1..m$, i.e. if it contains no subterm $\_j \,|\, a$ or $a \,|\, \_j$ for any j.

Labelled Transitions The labelled transitions will be of the same form as in the previous section, with transitions $s \xrightarrow{F} T$ for $s : 0 \to 1$, $F : 1 + n \to 1$ and $T : n \to 1$. A non-trivial label F may either contribute a deep subcontext of the left hand side of a rewrite rule (analogous to the non-identity labels of the previous section) or a parallel component, respectively with F deep or shallow in its first argument. The cases must be treated differently. For example, the rule

$$\alpha \,|\, \beta \longrightarrow \gamma$$

will generate labelled transitions

$$s \,|\, \alpha \xrightarrow{\_ \,|\, \beta} s \,|\, \gamma \qquad s \,|\, \beta \xrightarrow{\_ \,|\, \alpha} s \,|\, \gamma$$

for all $s : 0 \to 1$. As before, transitions that contribute the whole of the left hand side of a rule, such as $s \xrightarrow{\_ \,|\, \alpha \,|\, \beta} s \,|\, \gamma$, are redundant and will be excluded. It is necessary to take labels to be subcontexts of left hand sides of rules up to structural congruence, not merely up to equality. For example, given the rule

$$(\alpha \,|\, \beta) \,|(\gamma \,|\, \delta) \longrightarrow \epsilon$$

we need labelled transitions

$$\alpha \mid \gamma \mid r \xrightarrow{\_ \mid (\beta \mid \delta)} \epsilon \mid r$$

Finally, the existence of rules in which arguments occur in parallel with non-trivial terms means that we must deal with partially instantiated arguments. Consider the rule

$$\sigma(\tau(\_1) \mid \_3,\ \_2) \longrightarrow R$$

The term $\tau(\mu) \mid \rho$ could be placed in any context $\sigma(\_ \mid s,\ t)$ to create an instance of the left hand side, with μ (from the term) instantiating $\_1$, t (from the context) instantiating $\_2$, and $\rho \mid s$ (from both) instantiating $\_3$. There will be a labelled transition

$$\tau(\mu) \mid \rho \xrightarrow{\sigma(\_ \mid \_2,\ \_1)} R \cdot \langle \mu,\ \_1,\ \rho \mid \_2 \rangle_2$$

parametric in two places but partially instantiating the second by ρ. The general definition of transitions is given in Figure 3. It uses additional notation – we write $\mathbf{par}_n$ for $\langle \_1 \mid (\ldots \mid \_n) \rangle_n : n \to 1$ and $\mathbf{ppar}_n$ for $\langle \_1 \mid \_{n+1}, \ldots, \_n \mid \_{n+n} \rangle_{n+n} : n + n \to n$. Some parts of the definition are illustrated in Figure 4, in which rectangles denote contexts and terms, triangles denote instances of **par**, and hatched triangles denote instances of **ppar**.

To a first approximation, the definition for F deep in 1 states that $s \xrightarrow{F} T$ iff there is a rule $L \longrightarrow R$, with $L, R : m_1 + m_2 + m_3 \to 1$, such that L can be factored into L_2 (with m_2 arguments) enclosing L_1 (with m_1 arguments) in parallel with m_3 arguments. The source s is L_1 instantiated by u, in parallel with e; the label F is roughly L_2; the target T is R with m_1 arguments instantiated by u and m_3 partially instantiated by e.

The definition for F shallow in 1 states that $s \xrightarrow{F} T$ iff there is a rule $L \longrightarrow R$ such that L can be factored into L_1 (with m_1 arguments) in parallel with L_2 (with m_2 arguments) and with m_3 other arguments. The source s is L_1 instantiated by u, in parallel with e and with an arbitrary term q; the label F is roughly L_2; the target T is R with m_1 arguments instantiated by u and m_3 partially instantiated by e, again all in parallel with q. It is worth noting that the non-identity labelled transitions do not depend on the set of reduction contexts.

The intention is that the labelled transition relations provide just enough information so that the reductions of a term $A \cdot s$ are determined by the labelled transitions of s and the structure of A, which is the main property required for a congruence proof. The key lemma (Lemma 27, in Appendix C.2) involves a detailed analysis of possible occurrences of an instance $L \cdot u$ of the left hand side L of a rewrite rule within a term $A \cdot s$. Inspection of the proof of this

Transitions $s \xrightarrow{F} T$, for $s : 0 \to 1$, $F : 1{+}n \to 1$ linear and $T : n \to 1$, are defined by:

- For $F \equiv \mathbf{id}_1$: $s \xrightarrow{F} T$ iff

$$\exists \langle m, L, R \rangle \in \mathcal{R}, C \in \mathcal{C}, u : 0 \to m\,.\ \ s \equiv C \cdot L \cdot u \wedge C \cdot R \cdot u \equiv T$$

- For F deep in argument 1: $s \xrightarrow{F} T$ iff there exist

$\langle m, L, R \rangle \in \mathcal{R}$
m_1, m_2 and m_3 such that $m_1 + m_2 + m_3 = m$ and $n = m_3 + m_2$
$\pi : m \to m$ a permutation
$L_1 : m_1 \to 1$ linear and deep
$L_2 : 1 + m_2 \to 1$ linear, deep in argument 1 and 1-separated
$u : 0 \to m_1$
$e : 0 \to m_3$

such that

$$\begin{aligned}
&L \equiv L_2 \cdot (\mathbf{par}_{1+m_3} \cdot (L_1 + \mathbf{id}_{m_3}) + \mathbf{id}_{m_2}) \cdot \pi \\
&s \equiv \mathbf{par}_{1+m_3} \cdot (L_1 \cdot u + e) \\
&T \equiv R \cdot \pi^{-1} \cdot (u + \mathbf{ppar}_{m_3} \cdot (\mathbf{id}_{m_3} + e) + \mathbf{id}_{m_2}) \\
&F \equiv L_2 \cdot (\mathbf{par}_{1+m_3} + \mathbf{id}_{m_2}) \\
&m_3 = 1 \implies L_1 \not\equiv \langle 0 \rangle_0
\end{aligned}$$

- For F shallow in argument 1 and $F \not\equiv \mathbf{id}_1$: $s \xrightarrow{F} T$ iff there exist

$\langle m, L, R \rangle \in \mathcal{R}$
m_1, m_2 and m_3 such that $m_1 + m_2 + m_3 = m$ and $n = m_3 + m_2$
$\pi : m \to m$ a permutation
$q : 0 \to 1$
$L_1 : m_1 \to 1$ linear and deep
$L_2 : m_2 \to 1$ linear and deep
$u : 0 \to m_1$
$e : 0 \to m_3$

such that

$$\begin{aligned}
&L \equiv \mathbf{par}_{2+m_3} \cdot (L_1 + \mathbf{id}_{m_3} + L_2) \cdot \pi \\
&s \equiv \mathbf{par}_{2+m_3} \cdot (q + L_1 \cdot u + e) \\
&T \equiv \mathbf{par}_2 \cdot (q + R \cdot \pi^{-1} \cdot (u + \mathbf{ppar}_{m_3} \cdot (\mathbf{id}_{m_3} + e) + \mathbf{id}_{m_2})) \\
&F \equiv \mathbf{par}_{2+m_3} \cdot (\mathbf{id}_1 + \mathbf{id}_{m_3} + L_2) \\
&m_3 = 0 \implies L_1 \not\equiv \langle 0 \rangle_0
\end{aligned}$$

Fig. 3. Contextual Labelled Transitions

lemma may make it seem plausible that the labelled transitions provide no extraneous information, but a precise result would be desirable.

Bisimulation Congruence Bisimulation $\sim$ is defined exactly as in the previous section. As before, the congruence proof requires dissection lemmas, analogous to Lemmas 1 and 6, lemmas showing that if $A \cdot s$ has a transition then s has a related transition, analogous to Lemmas 2,3 and 7,8, and partial converses to these, analogous to Lemmas 4 and 9. All except the statement of the main dissection lemma are deferred to Appendix C.

Lemma 13 (Dissection) *If $m \geq 0$,*

$$\begin{array}{ll} A : 1 \to 1 & B : m \to 1 \\ a : 0 \to 1 & b : 0 \to m \end{array}$$

with A and B linear, and $A \cdot a \equiv B \cdot b$, then one of the following hold

(1) (a is not deeply in any component of b) There exist
m_1, m_2 and m_3 such that $m_1 + m_2 + m_3 = m$
$\pi_1 : m \to m_1$, $\pi_2 : m \to m_2$ and $\pi_3 : m \to m_3$ a partition
$C : 1 + m_2 \to 1$ linear and 1-separated
$D : m_1 \to 1$ linear and deep
$e_1 : 0 \to m_3$
$e_2 : 0 \to m_3$
such that

$$\begin{aligned} A &\equiv C \cdot (\mathbf{par}_{1+m_3} \cdot (\mathbf{id}_1 + e_2) + \pi_2 \cdot b) \\ a &\equiv \mathbf{par}_{1+m_3} \cdot (D \cdot \pi_1 \cdot b + e_1) \\ B &\equiv C \cdot (\mathbf{par}_{1+m_3} \cdot (D + \mathbf{id}_{m_3}) + \mathbf{id}_{m_2}) \cdot (\pi_1 \oplus \pi_3 \oplus \pi_2) \\ \pi_3 \cdot b &\equiv \mathbf{ppar}_{m_3} \cdot (e_1 + e_2) \end{aligned}$$

There are m_1 of the b in a, m_2 of the b in A and m_3 of the b potentially overlapping A and a. The latter are split into e_1, in a, and e_2, in A.

(2) (a is deeply in a component of b) $m \geq 1$ and there exist

$$\begin{array}{l} \pi_1 : m \to 1 \text{ and } \pi_2 : m \to (m-1) \text{ a partition} \\ E : 1 \to 1 \text{ linear and deep} \end{array}$$

such that

$$\begin{aligned} A &\equiv B \cdot (\pi_1 \oplus \pi_2)^{-1} \cdot (E + \pi_2 \cdot b) \\ E \cdot a &\equiv \pi_1 \cdot b \end{aligned}$$

The first clause of the lemma is illustrated in Figure 5. For example, consider $A \cdot a \equiv B \cdot b \equiv \sigma(\tau(\mu_1) \mid \rho_1 \mid \rho_2, \mu_2)$, where

$$\begin{array}{ll} A = \sigma(\_ \mid \rho_2, \mu_2) & B = \sigma(\tau(\_{1}) \mid \_{3}, \_{2}) \\ a = \tau(\mu_1) \mid \rho_1 & b = \langle \mu_1, \mu_2, \rho_1 \mid \rho_2 \rangle_0 \end{array}$$

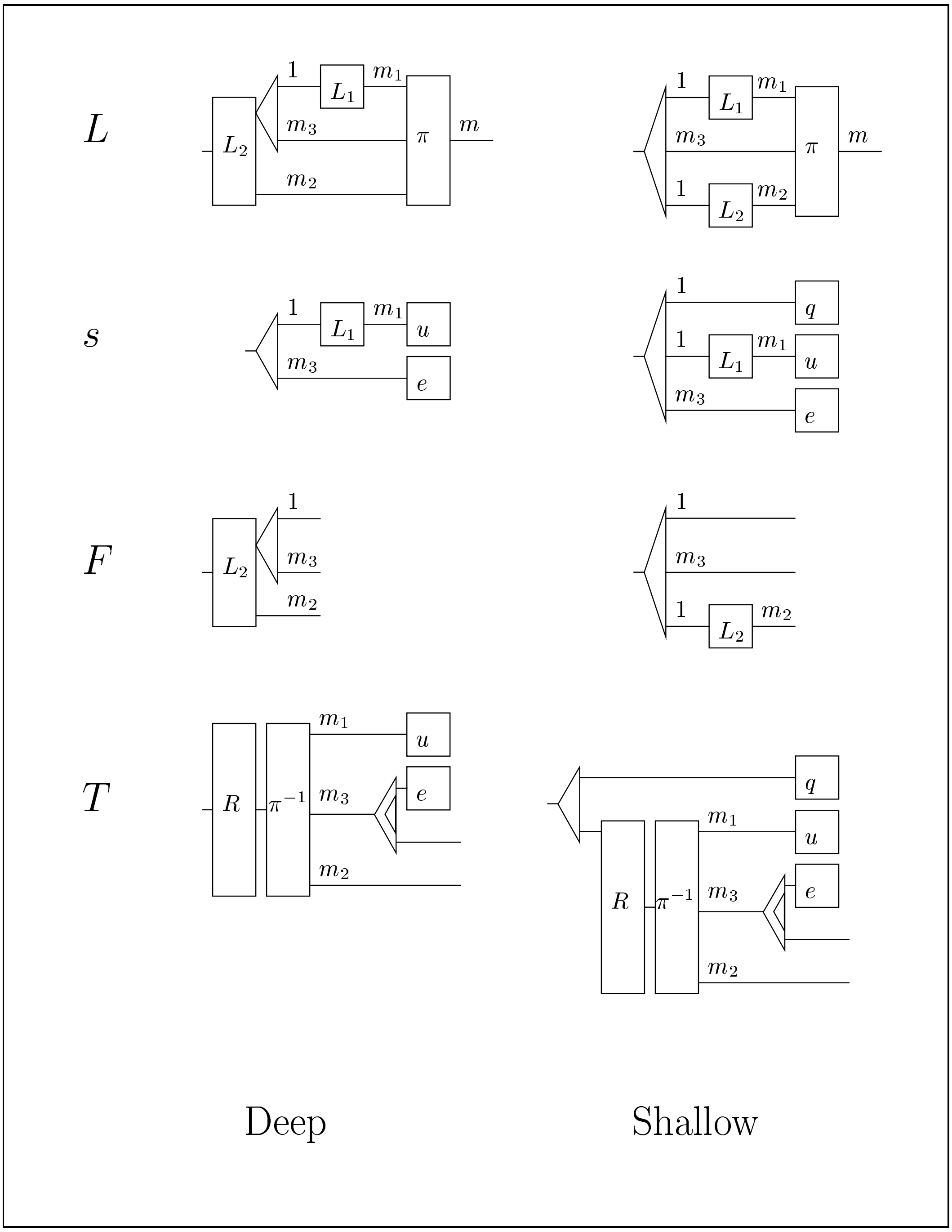

Fig. 4. Contextual Labelled Transitions Illustrated

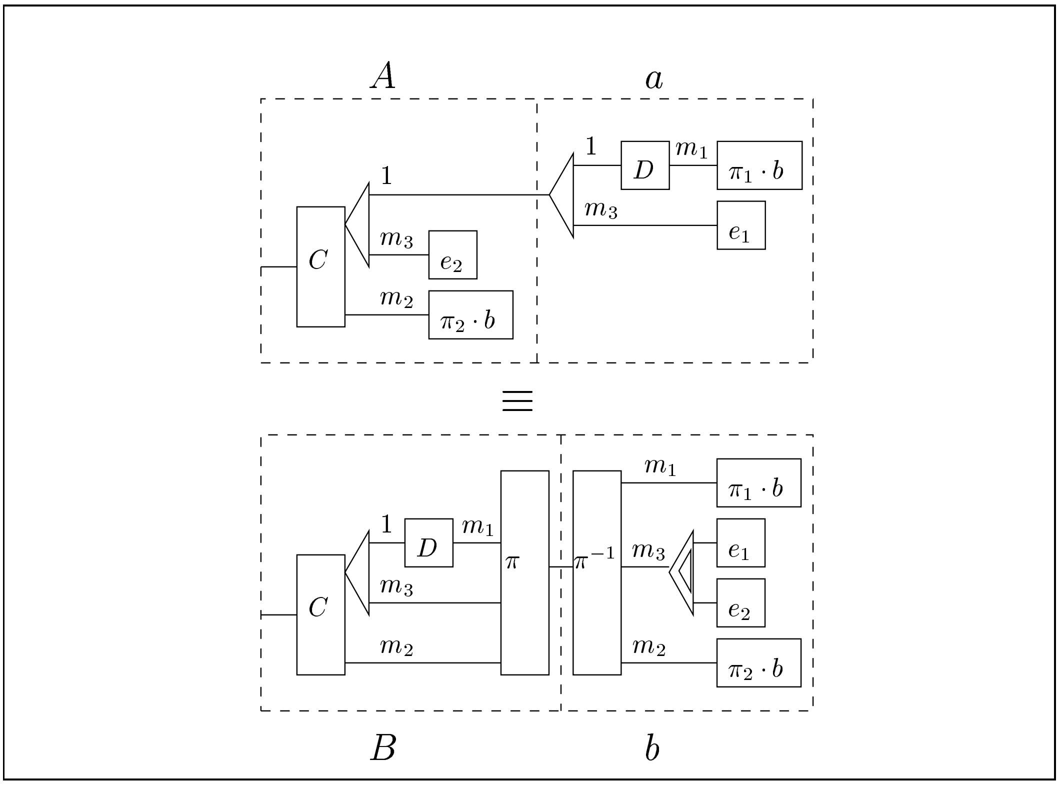

Fig. 5. Clause 1 of Dissection Lemma

Clause 1 of the lemma holds, with

$$\begin{aligned} C &= \sigma(_{-1}, _{-2}) & m &= 3 & \pi_1 &= \langle _{-1} \rangle_3 \\ D &= \tau(_{-1}) & m_1 &= 1 & \pi_2 &= \langle _{-2} \rangle_3 \\ e_1 &= \rho_1 & m_2 &= 1 & \pi_3 &= \langle _{-3} \rangle_3 \\ e_2 &= \rho_2 & m_3 &= 1 & & \\ \pi_1 \cdot b &= \mu_1 & & & & \\ \pi_2 \cdot b &= \mu_2 & & & & \end{aligned}$$

This dissection should give rise to a transition

$$\tau(\mu_1) \mid \rho_1 \xrightarrow{\sigma(\_ \mid _{-2}, _{-1})} R \cdot \langle \mu_1, _{-2}, _{-1} \mid \rho_1 \rangle_2$$

(taking A, a, B, b to be the D, s, L, u in case **i** of Lemma 27).

Theorem 14 $\sim$ *is a congruence.*

Proof We show that $(\equiv \mathcal{S})^*$, where

$$\mathcal{S} \stackrel{def}{=} \{ A \cdot s, A \cdot s' \mid s \sim s' \wedge A : 1 \to 1 \text{ linear} \}$$

is a bisimulation. As before, note that for any $A : 1 \to 1$ and $s \sim s'$ we have $A \cdot s \; \mathcal{S}^* \; A \cdot s'$. We first show that if $A : 1 \to 1$ linear, $s \sim s'$ and $A \cdot s \xrightarrow{F} T$ then there exists T' such that $A \cdot s' \xrightarrow{F} T'$ and $T \equiv [\mathcal{S}^*] \; T'$.

(1) Suppose $A \cdot s \xrightarrow{I} t$ and $I \equiv \mathbf{id}_1$. By Lemma 27 one of the following holds:

(a) There exists some $H : 1 \to 1$ such that $t \equiv H \cdot s$ and $\forall \hat{s} : 0 \to 1\,.\; A \cdot \hat{s} \xrightarrow{-} H \cdot \hat{s}$.

Hence $A \cdot s' \xrightarrow{-} H \cdot s'$.

Clearly $t \equiv H \cdot s \; \mathcal{S}^* \; H \cdot s'$.

(b) There exist $n \geq 0$, $F : (1+n) \to 1$ linear, $T : n \to 1$, $C \in \mathcal{C}$ and $v : 0 \to n$ such that $s \xrightarrow{F} T$, $A \equiv C \cdot F \cdot (\mathbf{id}_1 + v)$ and $t \equiv C \cdot T \cdot v$.

By $s \sim s'$ there exists T' such that $s' \xrightarrow{F} T' \wedge T \; [\sim] \; T'$.

By Lemma 30 $F \cdot (s' + v) \xrightarrow{-} T' \cdot v$.

By the definition of reduction $A \cdot s' \equiv C \cdot F \cdot (s' + v) \xrightarrow{-} C \cdot T' \cdot v$.

Clearly $t \equiv C \cdot T \cdot v \; \mathcal{S}^* \; C \cdot T' \cdot v$.

(2) Suppose $A \cdot s \xrightarrow{F} T$ for $A : 1 \to 1$ linear and $F : 1 + n \to 1$ linear and deep in 1. By Lemma 28 one of the following holds.

(a) There exists $H : 1 + n \to 1$ such that $T \equiv H \cdot (s + \mathbf{id}_n)$ and for all $\hat{s} : 0 \to 1$ we have $A \cdot \hat{s} \xrightarrow{F} H \cdot (\hat{s} + \mathbf{id}_n)$.

Hence $A \cdot s' \xrightarrow{F} H \cdot (s' + \mathbf{id}_n)$.

Clearly $T \equiv H \cdot (s + \mathbf{id}_n) \; [\mathcal{S}^*] \; H \cdot (s' + \mathbf{id}_n)$.

(b) There exist

$m_{13} \geq 0$ and $m_{12} \geq 0$ and $m_2 \geq 0$ and $m_3 \geq 0$
such that $n = m_3 + m_2$
$L_{12} : 1 + m_{12} \to 1$ linear, deep in 1 and 1-separated
$L_2 : 1 + m_2 \to 1$ linear, deep in argument 1 and 1-separated
$\hat{T} : m_{13} + m_{12} + m_3 + m_2 \to 1$
$v_3 : 0 \to m_{13}$
$v_2 : 0 \to m_{12}$
$e : 0 \to m_3$

such that

$$s \xrightarrow{L_2 \cdot (\mathbf{par}_{1+m_3} + \mathbf{id}_{m_2}) \cdot (L_{12} + \mathbf{id}_n) \cdot (\mathbf{par}_{1+m_{13}} + \mathbf{id}_{m_{12}+m_3+m_2})} \hat{T}$$
$$F \equiv L_2 \cdot (\mathbf{par}_{1+m_3} + \mathbf{id}_{m_2})$$
$$T \equiv \hat{T} \cdot (v_3 + v_2 + \mathbf{ppar}_{m_3} \cdot (e + \mathbf{id}_{m_3}) + \mathbf{id}_{m_2})$$
$$A \equiv \mathbf{par}_{1+m_3} \cdot (L_{12} \cdot (\mathbf{par}_{1+m_{13}} \cdot (\mathbf{id}_1 + v_3) + v_2) + e)$$

By $s \sim s'$ there exists $\hat{T}'$ such that $\hat{T} \; [\sim] \; \hat{T}'$ and

$$s' \xrightarrow{L_2 \cdot (\mathbf{par}_{1+m_3} + \mathbf{id}_{m_2}) \cdot (L_{12} + \mathbf{id}_n) \cdot (\mathbf{par}_{1+m_{13}} + \mathbf{id}_{m_{12}+m_3+m_2})} \hat{T}'$$

By Lemma 31 $A \cdot s' \xrightarrow{F} \hat{T}' \cdot (v_3 + v_2 + \mathbf{ppar}_{m_3} \cdot (e + \mathbf{id}_{m_3}) + \mathbf{id}_{m_2})$. Clearly $T \equiv \hat{T} \cdot (v_3 + v_2 + \mathbf{ppar}_{m_3} \cdot (e + \mathbf{id}_{m_3}) + \mathbf{id}_{m_2}) \; [\mathcal{S}^*] \; \hat{T}' \cdot (v_3 + v_2 + \mathbf{ppar}_{m_3} \cdot (e + \mathbf{id}_{m_3}) + \mathbf{id}_{m_2})$.

(c) There exist

$$\begin{array}{l} m_{12} \geq 0 \text{ and } m_2 \geq 0 \text{ and } m_3 \geq 0 \text{ such that } n = m_3 + m_2 \\ L_{12} : m_{12} \to 1 \text{ linear and deep} \\ L_2 : 1 + m_2 \to 1 \text{ linear, deep in argument 1 and 1-separated} \\ \hat{T} : m_3 + m_{12} + m_2 \to 1 \\ v : 0 \to m_{12} \\ \hat{\hat{a}} : 0 \to m_3 \end{array}$$

such that

$$\begin{array}{l} s \stackrel{L_2 \cdot (\mathbf{par}_{2+m_3} + \mathbf{id}_{m_2}) \cdot (\mathbf{id}_1 + \mathbf{id}_{m_3} + L_{12} + \mathbf{id}_{m_2})}{\longrightarrow} \hat{T} \\ F \equiv L_2 \cdot (\mathbf{par}_{1+m_3} + \mathbf{id}_{m_2}) \\ T \equiv \hat{T} \cdot (\mathbf{ppar}_{m_3} \cdot (\mathbf{id}_{m_3} + \hat{\hat{a}}) + v + \mathbf{id}_{m_2}) \\ A \equiv \mathbf{par}_{2+m_3} \cdot (\mathbf{id}_1 + L_{12} \cdot v + \hat{\hat{a}}) \end{array}$$

By $s \sim s'$ there exists $\hat{T}'$ such that $\hat{T} \, [\sim] \, \hat{T}'$ and

$$s' \stackrel{L_2 \cdot (\mathbf{par}_{2+m_3} + \mathbf{id}_{m_2}) \cdot (\mathbf{id}_1 + \mathbf{id}_{m_3} + L_{12} + \mathbf{id}_{m_2})}{\longrightarrow} \hat{T}'$$

By Lemma 32 $A \cdot s' \stackrel{F}{\longrightarrow} \hat{T}' \cdot (\mathbf{ppar}_{m_3} \cdot (\mathbf{id}_{m_3} + \hat{\hat{a}}) + v + \mathbf{id}_{m_2})$. Clearly $T \equiv \hat{T} \cdot (\mathbf{ppar}_{m_3} \cdot (\mathbf{id}_{m_3} + \hat{\hat{a}}) + v + \mathbf{id}_{m_2}) \, [\mathcal{S}^*] \, \hat{T}' \cdot (\mathbf{ppar}_{m_3} \cdot (\mathbf{id}_{m_3} + \hat{\hat{a}}) + v + \mathbf{id}_{m_2})$.

(3) Suppose $A \cdot s \stackrel{F}{\longrightarrow} T$ for $A : 1 \to 1$ linear and $F : 1 + n \to 1$ linear, shallow in 1 and $F \not\equiv \mathbf{id}_1$.

By Lemma 29 one of the following holds.

(a) There exists $H : 1 + n \to 1$ such that $T \equiv H \cdot (s + \mathbf{id}_n)$ and for all $\hat{s} : 0 \to 1$ we have $A \cdot \hat{s} \stackrel{F}{\longrightarrow} H \cdot (\hat{s} + \mathbf{id}_n)$.

Hence $A \cdot s' \stackrel{F}{\longrightarrow} H \cdot (s' + \mathbf{id}_n)$.

Clearly $T \equiv H \cdot (s + \mathbf{id}_n) \, [\mathcal{S}^*] \, H \cdot (s' + \mathbf{id}_n)$.

(b) There exist

$$\begin{array}{l} m_{13} \geq 0 \text{ and } m_{12} \geq 0 \text{ and } m_2 \geq 0 \text{ and } m_3 \geq 0 \\ \qquad \text{such that } n = m_3 + m_2 \\ q : 0 \to 1 \\ L_{12} : 1 + m_{12} \to 1 \text{ linear, deep and 1-separated} \\ L_2 : m_2 \to 1 \text{ linear and deep} \\ \hat{T} : m_{13} + m_{12} + m_3 + m_2 \to 1 \\ v_3 : 0 \to m_{13} \\ v_2 : 0 \to m_{12} \\ e : 0 \to m_3 \end{array}$$

such that

$$s \stackrel{\mathbf{par}_{2+m_3}\cdot(L_{12}+\mathbf{id}_{m_3}+L_2)\cdot(\mathbf{par}_{1+m_{13}}+\mathbf{id}_{m_{12}+m_3+m_2})}{\longrightarrow} \hat{T}$$
$$F \equiv \mathbf{par}_{2+m_3}\cdot(\mathbf{id}_1 + \mathbf{id}_{m_3} + L_2)$$
$$T \equiv \mathbf{par}_2\cdot(q + \hat{T}\cdot(v_3 + v_2 + \mathbf{ppar}_{m_3}\cdot(e + \mathbf{id}_{m_3}) + \mathbf{id}_{m_2}))$$
$$A \equiv \mathbf{par}_{2+m_3}\cdot(q + L_{12}\cdot(\mathbf{par}_{1+m_{13}}\cdot(\mathbf{id}_1 + v_3) + v_2) + e)$$
$$m_3 = 0 \implies L_2 \not\equiv \langle 0\rangle_0$$

By $s \sim s'$ there exists $\hat{T}'$ such that $\hat{T}\ [\sim]\ \hat{T}'$ and

$$s' \stackrel{\mathbf{par}_{2+m_3}\cdot(L_{12}+\mathbf{id}_{m_3}+L_2)\cdot(\mathbf{par}_{1+m_{13}}+\mathbf{id}_{m_{12}+m_3+m_2})}{\longrightarrow} \hat{T}'$$

By Lemma 33 $A \cdot s' \stackrel{F}{\longrightarrow} \mathbf{par}_2\cdot(q + \hat{T}'\cdot(v_3 + v_2 + \mathbf{ppar}_{m_3}\cdot(e + \mathbf{id}_{m_3}) + \mathbf{id}_{m_2}))$. Clearly $T \equiv \mathbf{par}_2\cdot(q + \hat{T}\cdot(v_3 + v_2 + \mathbf{ppar}_{m_3}\cdot(e + \mathbf{id}_{m_3}) + \mathbf{id}_{m_2}))\ [\mathcal{S}^*]\ \mathbf{par}_2\cdot(q + \hat{T}'\cdot(v_3 + v_2 + \mathbf{ppar}_{m_3}\cdot(e + \mathbf{id}_{m_3}) + \mathbf{id}_{m_2}))$.

(c) There exist

$m_{12} \geq 0$ and $m_2 \geq 0$ and $m_3 \geq 0$ such that $n = m_3 + m_2$
$a' : 0 \to 1$
$L_{12} : m_{12} \to 1$ linear and deep
$L_2 : m_2 \to 1$ linear and deep
$\hat{T} : m_3 + m_{12} + m_2 \to 1$
$v_2 : 0 \to m_{12}$
$a''' : 0 \to m_3$

such that

$$s \stackrel{\mathbf{par}_{3+m_3}\cdot(\mathbf{id}_1+\mathbf{id}_{m_3}+L_{12}+L_2)}{\longrightarrow} \hat{T}$$
$$F \equiv \mathbf{par}_{2+m_3}\cdot(\mathbf{id}_1 + \mathbf{id}_{m_3} + L_2)$$
$$T \equiv \mathbf{par}_2\cdot(a' + \hat{T}\cdot(\mathbf{ppar}_{m_3}\cdot(\mathbf{id}_{m_3} + a''') + v_2 + \mathbf{id}_{m_2}))$$
$$A \equiv \mathbf{par}_{1+2+m_3}\cdot(\mathbf{id}_1 + a' + L_{12}\cdot v_2 + a''')$$
$$m_3 = 0 \implies L_2 \not\equiv \langle 0\rangle_0$$

By $s \sim s'$ there exists $\hat{T}'$ such that $\hat{T}\ [\sim]\ \hat{T}'$ and

$$s' \stackrel{\mathbf{par}_{3+m_3}\cdot(\mathbf{id}_1+\mathbf{id}_{m_3}+L_{12}+L_2)}{\longrightarrow} \hat{T}'$$

By Lemma 34 $A \cdot s' \stackrel{F}{\longrightarrow} \mathbf{par}_2\cdot(a' + \hat{T}'\cdot(\mathbf{ppar}_{m_3}\cdot(\mathbf{id}_{m_3} + a''') + v_2 + \mathbf{id}_{m_2}))$. Clearly $T \equiv \mathbf{par}_2\cdot(a' + \hat{T}\cdot(\mathbf{ppar}_{m_3}\cdot(\mathbf{id}_{m_3} + a''') + v_2 + \mathbf{id}_{m_2}))\ [\mathcal{S}^*]\ \mathbf{par}_2\cdot(a' + \hat{T}'\cdot(\mathbf{ppar}_{m_3}\cdot(\mathbf{id}_{m_3} + a''') + v_2 + \mathbf{id}_{m_2}))$.

Now if

$$r_1 \equiv A_1 \cdot s_1\ \mathcal{S}\ A_1 \cdot s_2' \equiv A_2 \cdot s_2\ \mathcal{S}\ \ldots\ \mathcal{S}\ A_{n-1} \cdot s_n'$$

for A_i linear and $s_i \sim s'_{i+1}$, for $i \in 1..n-1$, and $r_1 \xrightarrow{F} T_1$ then by the closure of transitions under $\equiv$, and the above, there exists T_n such that $A_{n-1} \cdot s'_n \xrightarrow{F} T_n$ and $T_1 \; [(\equiv \mathcal{S})^*] \; T_n$.

$\square$

Remark The definitions allow only rather crude specifications of the set $\mathcal{C}$ of reduction contexts. They ensure that $\mathcal{C}$ has a number of closure properties, which are used in the proof of Lemma 27 (in Appendix C.2). Some reduction semantics require more delicate sets of reduction contexts. For example, for a list cons constructor one might want to allow reduction contexts cons($\_, e$) and cons($v, \_$), where e is arbitrary but v ranges only over some given set of *values*. This would require a non-trivial generalisation of the theory.

Example – CCS synchronization For our CCS fragment the definition gives

$$\begin{array}{l} \alpha.u \,|\, r \xrightarrow{\_|\, \bar{\alpha}.\_1} u \,|\, \_1 \,|\, r \\ \bar{\alpha}.u \,|\, r \xrightarrow{\_|\, \alpha.\_1} u \,|\, \_1 \,|\, r \end{array}$$

together with structurally congruent transitions, i.e. those generated by

$$\frac{s' \equiv s \quad s \xrightarrow{F} T \quad T \equiv T' \quad F \equiv F'}{s' \xrightarrow{F'} T'}$$

and the reductions.

Proposition 15 $\sim$ *coincides with bisimulation over the labelled transitions of Section 1.*

Proof Write $\sim_{\text{std}}$ for the standard bisimulation over the labelled transitions of Section 1. To show $\sim_{\text{std}}$ is a bisimulation for the contextual labelled transitions, suppose $P \sim_{\text{std}} P'$ and $P \xrightarrow{\_|\, \bar{\alpha}.\_1} T$. There must exist u and r such that $P \equiv \alpha.u \,|\, r$ and $T \equiv u \,|\, \_1 \,|\, r$, but then $P \xrightarrow{\alpha} \equiv u \,|\, r$, so there exists Q' such that $P' \xrightarrow{\alpha} Q' \sim_{\text{std}} u \,|\, r$. There must then exist u' and r' such that $P' \equiv \alpha.u' \,|\, r'$ and $Q \equiv u' \,|\, r'$, hence $P' \xrightarrow{\_|\, \bar{\alpha}.\_1} u' \,|\, \_1 \,|\, r'$. Using the fact that $\sim_{\text{std}}$ is a congruence we have $\forall s \,.\; u \,|\, s \,|\, r \sim_{\text{std}} u' \,|\, s \,|\, r$ so $T \; [\sim_{\text{std}}] \; u' \,|\, \_1 \,|\, r'$.

For the converse, suppose $P \sim P'$ and $P \xrightarrow{\alpha} Q$. There must exist u and r such that $P \equiv \alpha.u \,|\, r$ and $Q \equiv u \,|\, r$, but then $P \xrightarrow{\_|\, \bar{\alpha}.\_1} u \,|\, \_1 \,|\, r$, so there exists T' such that $P' \xrightarrow{\_|\, \bar{\alpha}.\_1} T' \wedge (u \,|\, \_1 \,|\, r) \; [\sim] \; T'$. There must then exist u' and r' such that $P' \equiv \alpha.u' \,|\, r'$ and $T' \equiv u' \,|\, \_1 \,|\, r'$, hence $P' \xrightarrow{\alpha} u' \,|\, r'$. By the definition of [ ] we have $P' \equiv u \,|\, 0 \,|\, r \sim u' \,|\, 0 \,|\, r'$. $\square$

The standard transitions coincide (modulo structural congruence) with the contextual labelled transitions with their parameter instantiated by 0. One might look for general conditions on $\mathcal{R}$ under which bisimulation over such 0-instantiated transitions is already a congruence, and coincides with $\sim$.

Example – Ambient movement The CCS fragment is degenerate in several respects – in the left hand side of the rewrite rule there are no nested non-parallel symbols and no parameters in parallel with any non-0 term, so there are no deep transitions and no partial instantiations. As a less degenerate example we consider a fragment of the Ambient Calculus [10] without binding. The theory gives rise to a labelled transition relation and bisimulation congruence that appear plausible, though we leave an exact comparison with the bisimulation in [10] to future work. The signature Σ_{Amb} has unary $m[\;]$ (written outfix), in $m.$, out $m.$ and open $m.$, for all $m \in \mathcal{A}$. Of these only the $m[\;]$ allow reduction. The rewrite rules $\mathcal{R}_{\mathrm{Amb}}$ are

$$\begin{aligned} n[\mathrm{in}\ m.\_1 \mid \_2] \mid m[\_3] &\longrightarrow m[n[\_1 \mid \_2] \mid \_3] \\ m[n[\mathrm{out}\ m.\_1 \mid \_2] \mid \_3] &\longrightarrow n[\_1 \mid \_2] \mid m[\_3] \\ \mathrm{open}\ m.\_1 \mid m[\_2] &\longrightarrow \_1 \mid \_2 \end{aligned}$$

The definition gives the transitions below, together with structurally congruent transitions, permutation instances, and the reductions.

$$\begin{aligned} \mathrm{in}\ m.s \mid r &\xrightarrow{n[\_ \mid \_1] \mid m[\_2]} m[n[s \mid r \mid \_1] \mid \_2] \\ n[\mathrm{in}\ m.s \mid t] \mid r &\xrightarrow{\_ \mid m[\_1]} m[n[s \mid t] \mid \_1] \mid r \\ m[s] \mid r &\xrightarrow{n[\mathrm{in}\ m.\_1 \mid \_2] \mid \_} m[n[\_1 \mid \_2] \mid s] \mid r \\ \mathrm{out}\ m.s \mid r &\xrightarrow{m[n[\_ \mid \_1] \mid \_2]} n[s \mid r \mid \_1] \mid m[\_2] \\ n[\mathrm{out}\ m.s \mid t] \mid r &\xrightarrow{m[\_ \mid \_1]} n[s \mid t] \mid m[r \mid \_1] \\ \mathrm{open}\ n.s \mid r &\xrightarrow{\_ \mid n[\_1]} s \mid \_1 \mid r \\ n[s] \mid r &\xrightarrow{\mathrm{open}\ n.\_1 \mid \_} \_1 \mid s \mid r \end{aligned}$$

5 Conclusion

We have given general definitions of contextual labelled transitions, and bisimulation congruence results, for three simple classes of reduction semantics. It is preliminary work – the definitions may inform work on particular interesting calculi, but to directly apply the results they must be generalized to more expressive classes of reduction semantics. Several directions are suggested below.

There is, of course, no guarantee that for any particular calculus the bisimulation given by the general theory will be satisfactory. The CCS example may be suggestively positive, but the fact that different sets of reduction rules (defining the same reduction relation) can give rise to different bisimulation relations implies that in some cases the bisimulation is bound not to be desirable. Examination of more serious examples is required. Moreover, any general theory is liable to involve heavier notation than work on a single particular calculus, where one can finely tune the notation and definitions – one might well expect to have to hand-optimise the general labelled transitions produced for a particular calculus in order to obtain a tractable set.

Colouring The definition of labelled transitions in Section 4 is rather intricate – for tractable generalisations, to more expressive settings, one would like a more concise characterisation. A promising approach seems to be to work with *coloured terms*, in which each symbol except $|$ and 0 is given a tag from a set of colours. This gives a notion of occurrence of a symbol in a term that is preserved by structural congruence and context application, and hence provides a different way of formalising the idea that the label of a transition $s \xrightarrow{F} T$ must be part of a redex within $F \cdot s$. For the case of ground term rewriting with parallel one can define labelled transitions by

- $s \xrightarrow{F} t \overset{def}{\Leftrightarrow} \exists \langle l, r \rangle \in \mathcal{R}, \boldsymbol{s}, D : 1 \rightarrow 1 \text{ linear}. \quad F^{\mathsf{red}} \cdot \boldsymbol{s} \equiv D^{\mathsf{blue}} \cdot l^{\mathsf{red}} \wedge |\boldsymbol{s}| \equiv s \wedge t \equiv D \cdot r$

where bold $\boldsymbol{s}$ ranges over terms of the coloured signature, superscripts colour all the symbols in the uncoloured term to which they are applied, and $|\_|$ removes colour tags. This appears to give rise to satisfactory bisimulation congruences, with essentially the same labelled transitions as the definition of Section 4 restricted to the ground case.

Summation The definitions and results of Section 4 are for signatures with a single ACI operator, which allow the reduction semantics of the CCS fragment

$$P ::= 0 \mid \alpha.P \mid \bar{\alpha}.P \mid P \,|\, P \qquad \alpha \in \mathcal{A}$$

to be expressed. To express the reduction semantics of the fragment with summation

$$P ::= 0 \mid \alpha.P \mid \bar{\alpha}.P \mid P \,|\, P \mid P + P \qquad \alpha \in \mathcal{A}$$

requires two ACI operators (with + blocking); the reduction rules are then

$$(\bar{\alpha}.P + Q) \,|\, (\alpha.P' + Q') \longrightarrow P \,|\, P'$$

Extending the theory to a class of signatures including this would involve new dissection results.

Higher order rewriting Functional programming languages can generally be equipped with straightforward definitions of operational congruence, involving quantification over contexts. As discussed in the introduction, in several cases these have been given tractable characterisations in terms of bisimulation. One might generalise the term rewriting case of Section 3 to some notion of higher order rewriting [42] equipped with non-trivial sets of reduction contexts, to investigate the extent to which this can be done uniformly.

Name binding To express calculi with mobile scopes, such as the π-calculus and its descendants, one requires a syntax with name binding, and a structural congruence allowing scope extrusion. Generalising the definitions of Section 4 to the class of all non-higher-order action calculi would take in a number of examples, some of which currently lack satisfactory operational congruences, and should show how the indexed structure of π labelled transitions arises from the rewrite rules and structural congruence.

Ultimately one would like to treat concurrent functional languages. In particular cases it has been shown that one can define labelled transitions that give rise to bisimulation congruences, e.g. by Ferreira, Hennessy and Jeffrey for Core CML [16]. To express the reduction semantics of such languages would require both higher order rules and a rich structural congruence.

Observational congruences We have focussed on strong bisimulation, which is a very intensional equivalence. It would be interesting to know the extent to which congruence proofs can be given uniformly for equivalences that abstract from branching time, internal reductions etc. More particularly, one would like to know whether Theorem 12 holds without the restriction to right-affine rewrite rules. As usual, one would expect bisimulation to differ from any truly observational equivalence for a programming language. It is arguable, however, that it will always be finer – if the language primitives for external input and output are designed to appear (from inside the language) just as other internal interactions, then the contextual labelled transitions should carry enough information. On a related note, one can define *barbs* for an arbitrary calculus by $s\downarrow \iff \exists F \not\equiv \mathbf{id}_1, T\ .\ \ s \xrightarrow{F} T$, so $s\downarrow$ iff s has some potential interaction with a context. Conditions under which this barbed bisimulation congruence coincides with $\sim$ could provide a useful test of the expressiveness of calculi.

Structural operational semantics This work has taken reduction semantics as primary, showing how labelled transition relations can be defined from a set of reduction rules. These definitions are not, however, inductive on term structure – we have not constructed an SOS from a set of reduction rules. Several authors taken labelled transitions as primary, considering calculi equipped with labelled transitions defined by an SOS in some well-behaved format; c.f. among others [3,6,8,13,18,23,41]. The relationship between the two is unclear

– one would like conditions on rewrite rules that ensure the labelled transitions of Section 4 are definable by a functorial operational semantics [41]. Conversely, one would like conditions on an SOS ensuring that it is characterised by a reduction semantics. General congruence results have also been given for calculi with semantics given by open-map-preserving functors, e.g. in [11]. Again, the relationship with the present work requires study.

Acknowledgements The author would like to thank Robin Milner, Philippa Gardner, Ole Jensen, Søren Lassen, Jamey Leifer, Jean-Jacques Lévy, and the anonymous referees, for many interesting discussions and comments, and to acknowledge support from EPSRC grants GR/K 38403 and GR/L 62290 and a Royal Society University Research Fellowship.

A Proofs for Section 2

For the inclusion of $\sim$ in $\sim_{\text{alt}}$:

Proposition 16 *If $s \sim t$ then $s \sim_{\text{alt}} t$.*

Proof It is straightforward to show that $\{ s, s' \mid s \sim s' \}$ is a bisimulation with respect to $\xrightarrow{F}_{\text{alt}}$. □

For the example showing the non-inclusion, the terms are $\gamma^n(\alpha)$ and $\gamma^n(\beta)$ for $n \geq 0$. The transitions are

$$
\begin{aligned}
\gamma^n(\alpha) &\xrightarrow{-} \gamma^n(\alpha) \\
\gamma^n(\beta) &\xrightarrow{-} \gamma^n(\beta) \\
\gamma^n(\beta) &\xrightarrow{-} \gamma^{n-1}(\beta) \text{ if } n \geq 1 \\
\beta &\xrightarrow{\gamma(-)} \beta
\end{aligned}
$$

so $\alpha \not\sim \beta$ whereas the alternative transitions are

$$
\begin{array}{ll}
\gamma^n(\alpha) \xrightarrow{-}_{\text{alt}} \gamma^n(\alpha) & \gamma^n(\alpha) \xrightarrow{\gamma(-)}_{\text{alt}} \gamma^{1+n}(\alpha) \\
\gamma^n(\beta) \xrightarrow{-}_{\text{alt}} \gamma^n(\beta) & \gamma^n(\beta) \xrightarrow{\gamma(-)}_{\text{alt}} \gamma^{1+n}(\beta) \\
\gamma^n(\beta) \xrightarrow{-}_{\text{alt}} \gamma^{n-1}(\beta) \text{ if } n \geq 1 & \gamma^n(\beta) \xrightarrow{\gamma(-)}_{\text{alt}} \gamma^n(\beta)
\end{array}
$$

(considering only those from the cut-down label set) so $\alpha \sim_{\text{alt}} \beta$.

B Proofs for Section 3

Proof of Lemma 6 The proof is by induction on the structure of A and B. $\square$

Proof of Lemma 7 By the definition of labelled transitions

$$\exists \langle m, L, R\rangle \in \mathcal{R}, C : 1 \to 1 \text{ linear}, u : 0 \to m \,.\; A \cdot s = C \cdot L \cdot u \wedge C \cdot R \cdot u = t$$

Applying Lemma 1 to $A \cdot s = C \cdot (L \cdot u)$ gives the following cases.

(1) ($L \cdot u$ is in s) There exists $B : 1 \to 1$ linear such that $s = B \cdot L \cdot u$ and $A \cdot B = C$. Taking $k = 0$, $F = \mathbf{id}_1$, $T = B \cdot R \cdot u$, $D = A$ and $v = \langle\rangle_0$ the second clause holds.

(2) (s is properly in $L \cdot u$) There exists $B : 1 \to 1$ linear with $B \neq \_$ such that $B \cdot s = L \cdot u$ and $A = C \cdot B$. Applying Lemma 6 to $B \cdot s = L \cdot u$ one of the following hold.

(a) (s is not in any component of u) There exist

$$\begin{array}{l} m_1 \text{ and } m_2 \text{ such that } m_1 + m_2 = m \\ \pi_i : m \to m_i \text{ for } i \in \{1, 2\} \text{ a partition} \\ F : 1 + m_2 \to 1 \text{ linear} \\ G : m_1 \to 1 \text{ linear and not the identity} \end{array}$$

such that

$$\begin{array}{rcl} B & = & F \cdot (\mathbf{id}_1 + \pi_2 \cdot u) \\ s & = & G \cdot \pi_1 \cdot u \\ L & = & F \cdot (G + \mathbf{id}_{m_2}) \cdot (\pi_1 \oplus \pi_2) \end{array}$$

i.e. there are m_1 components of u in s and m_2 in B. Taking $k = m_2$, $T = R \cdot (\pi_1 \oplus \pi_2)^{-1} \cdot (\pi_1 \cdot u + \mathbf{id}_{m_2})$, $D = C$ and $v = \pi_2 \cdot u$ the second clause holds. By $B \neq \mathbf{id}_1$ we know $F \neq \mathbf{id}_1$. There is a transition

$$s \xrightarrow{F} R \cdot (\pi_1 \oplus \pi_2)^{-1} \cdot (\pi_1 \cdot u + \mathbf{id}_{m_2})$$

with witness

$$\begin{array}{l} \langle m, L, R\rangle \in \mathcal{R} \\ m_1 \text{ and } m_2 \text{ such that } m_1 + m_2 = m \\ (\pi_1 \oplus \pi_2) : m \to m \text{ a permutation} \\ G : m_1 \to 1 \text{ linear and not the identity} \\ F : 1 + m_2 \to 1 \text{ linear and not the identity} \\ \pi_1 \cdot u : 0 \to m_1 \end{array}$$

(b) (s is in a component of u) $m \geq 1$ and there exist

$$\pi_1 : m \to 1 \text{ and } \pi_2 : m \to (m-1) \text{ a partition}$$
$$F : 1 \to 1 \text{ linear}$$

such that

$$B = L \cdot (\pi_1 \oplus \pi_2)^{-1} \cdot (F + \pi_2 \cdot u)$$
$$F \cdot s = \pi_1 \cdot u$$

Taking $H = C \cdot R \cdot (\pi_1 \oplus \pi_2)^{-1} \cdot (F + \pi_2 \cdot u)$ the first clause holds.

(3) (s and $L \cdot u$ are disjoint) There exists $E : 2 \to 1$ linear such that $A = E \cdot (\_ + L \cdot u)$ and $C = E \cdot (s + \_)$. Taking $H = E \cdot (\_ + R \cdot u)$ the first clause holds.

□

Proof of Lemma 8 By the definition of labelled transitions there exist

$$\langle m, L, R \rangle \in \mathcal{R} \text{ with } m \geq n$$
$$\pi : m \to m \text{ a permutation}$$
$$L_1 : (m-n) \to 1 \text{ linear and not the identity}$$
$$u : 0 \to (m-n)$$

such that

$$L = F \cdot (L_1 + \mathbf{id}_n) \cdot \pi$$
$$A \cdot s = L_1 \cdot u$$
$$T = R \cdot \pi^{-1} \cdot (u + \mathbf{id}_n)$$

Let $m_1 = m - n$ and $m_2 = n$. Applying Lemma 6 to $A \cdot s = L_1 \cdot u$ one of the following hold.

(1) (s is not in any component of u) There exist

$$m_{11} \text{ and } m_{12} \text{ such that } m_{11} + m_{12} = m_1$$
$$\theta_i : m_1 \to m_{1i} \text{ for } i \in \{1, 2\} \text{ a partition}$$
$$E : 1 + m_{12} \to 1 \text{ linear}$$
$$G : m_{11} \to 1 \text{ linear and not the identity}$$

such that

$$A = E \cdot (\mathbf{id}_1 + \theta_2 \cdot u)$$
$$s = G \cdot \theta_1 \cdot u$$
$$L_1 = E \cdot (G + \mathbf{id}_{m_{12}}) \cdot (\theta_1 \oplus \theta_2)$$

i.e. there are m_{11} components of u in s and m_{12} in A. Taking $p = m_{12}$, $\hat{T} = R \cdot ((\theta_1 \oplus \theta_2 + \mathbf{id}_{m_2}) \cdot \pi)^{-1} \cdot (\theta_1 \cdot u + \mathbf{id}_{m_{12}} + \mathbf{id}_{m_2})$ and $v = \theta_2 \cdot u$ we have clause 2. There is a transition

$$G \cdot \theta_1 \cdot u \stackrel{F \cdot (E + \mathbf{id}_n)}{\longrightarrow} R \cdot ((\theta_1 \oplus \theta_2 + \mathbf{id}_{m_2}) \cdot \pi)^{-1} \cdot (\theta_1 \cdot u + \mathbf{id}_{m_{12}} + \mathbf{id}_{m_2})$$

with witness

$\langle m, L, R \rangle \in \mathcal{R}$
m_{11} and $m_{12} + m_2$ such that $m_{11} + m_{12} + m_2 = m$
$((\theta_1 \oplus \theta_2 + \mathbf{id}_{m_2}) \cdot \pi) : m \to m$ a permutation
$G : m_{11} \to 1$ linear and not the identity
$F \cdot (E + \mathbf{id}_n) : 1 + m_{12} + m_2 \to 1$ linear and not the identity
$\theta_1 \cdot u : 0 \to m_{11}$

(2) (s is in a component of u) $m_1 \geq 1$ and there exist

$\theta_1 : m_1 \to 1$ and $\theta_2 : m_1 \to (m_1 - 1)$ a partition
$J : 1 \to 1$ linear

such that

$$A = L_1 \cdot (\theta_1 \oplus \theta_2)^{-1} \cdot (J + \theta_2 \cdot u)$$
$$J \cdot s = \theta_1 \cdot u$$

Taking $H = R \cdot \pi^{-1} \cdot ((\theta_1 \oplus \theta_2)^{-1} \cdot (J + \theta_2 \cdot u) + \mathbf{id}_{m_2})$ we have clause 1. There is a transition

$$A \cdot \hat{s} \stackrel{F}{\longrightarrow} R \cdot \pi^{-1} \cdot ((\theta_1 \oplus \theta_2)^{-1} \cdot (J + \theta_2 \cdot u) + \mathbf{id}_{m_2}) \cdot (\hat{s} + \mathbf{id}_{m_2})$$

with witness

$\langle m, L, R \rangle \in \mathcal{R}$
m_1 and m_2 such that $m_1 + m_2 = m$
$\pi : m \to m$ a permutation
$L_1 : m_1 \to 1$ linear and not the identity
$F : 1 + m_2 \to 1$ linear and not the identity
$(\theta_1 \oplus \theta_2)^{-1} \cdot (J \cdot \hat{s} + \theta_2 \cdot u) : 0 \to m_1$

□

Proof of Lemma 9 There are three cases. Firstly, suppose $p + n = 0$ and $C \cdot (E + \mathbf{id}_n) = \mathbf{id}_1$. It must then be that $C = \mathbf{id}_1$ and $E = \mathbf{id}_1$, so the conclusion is trivially true. Otherwise, by the definition of labelled transitions there exist

$\langle m, L, R \rangle \in \mathcal{R}$ with $m \geq (p + n)$
$\pi : m \to m$ a permutation
$L_1 : (m - (p + n)) \to 1$ linear and not the identity
$u : 0 \to (m - (p + n))$

such that

$$\begin{aligned} L &= C\cdot(E+\mathbf{id}_n)\cdot(L_1+\mathbf{id}_{(p+n)})\cdot\pi \\ s &= L_1\cdot u \\ T &= R\cdot\pi^{-1}\cdot(u+\mathbf{id}_{(p+n)}) \end{aligned}$$

Consider arbitrary $v:0\to p$.

(1) Case $C=\mathbf{id}_1$. Here $n=0$ so

$$\begin{aligned} E\cdot(s+v) &= L\cdot\pi^{-1}\cdot(u+v) \\ &\longrightarrow R\cdot\pi_2^{-1}\cdot(u+v) \\ &= T\cdot v \end{aligned}$$

(2) Case $C\neq\mathbf{id}_1$. There is a transition

$$E\cdot(s+v)\xrightarrow{C}T\cdot(v+\mathbf{id}_n)$$

with witness

$\langle m,L,R\rangle\in\mathcal{R}$
$(m-n)$ and n such that $(m-n)+n=m$
$\pi:m\to m$ a permutation
$E\cdot(L_1+\mathbf{id}_p):(m-n)\to 1$ linear and not the identity
$C:1+n\to 1$ linear and not the identity
$(u+v):0\to(m-n)$

□

Proof of Proposition 11 We check $\sim_{\mathcal{R}}$ is a bisimulation for the transitions $\xrightarrow{F}_{\mathrm{Cl}(\mathcal{R})}$. Consider $s\sim_{\mathcal{R}}s'$.

(1) Suppose $s\xrightarrow{-}_{\mathrm{Cl}(\mathcal{R})}t$. Trivially $s\xrightarrow{-}_{\mathcal{R}}t$. By $s\sim_{\mathcal{R}}s'$ there exists t' such that $s'\xrightarrow{-}_{\mathcal{R}}t'$ and $t\sim_{\mathcal{R}}t'$. Trivially $s'\xrightarrow{-}_{\mathrm{Cl}(\mathcal{R})}t'$.
(2) Suppose $s\xrightarrow{F}_{\mathrm{Cl}(\mathcal{R})}t$ and $F\neq\mathbf{id}_1$. By definition there exist $\langle m,L,R\rangle\in\mathcal{R}$ and $v:0\to m$ such that $F\cdot s=L\cdot v$ and $R\cdot v=t$. Applying Lemma 6 one of the following hold.
    (a) (s is not in any component of v) There exist

    m_1 and m_2 such that $m_1+m_2=m$
    $\pi_i:m\to m_i$ for $i\in\{1,2\}$ a partition
    $C:1+m_2\to 1$ linear
    $D:m_1\to 1$ linear and not the identity

    such that

$$\begin{aligned} F &= C\cdot(\mathbf{id}_1+\pi_2\cdot v) \\ s &= D\cdot\pi_1\cdot v \\ L &= C\cdot(D+\mathbf{id}_{m_2})\cdot(\pi_1\oplus\pi_2) \end{aligned}$$

i.e. there are m_1 components of v in s and m_2 in F. Here $s \xrightarrow{C}_{\mathcal{R}} R \cdot (\pi_1 \oplus \pi_2)^{-1} \cdot (\pi_1 \cdot v + \mathbf{id}_{m_2})$. By $s \sim_{\mathcal{R}} s'$ there exists T' such that $s' \xrightarrow{C}_{\mathcal{R}} T'$ and $R \cdot (\pi_1 \oplus \pi_2)^{-1} \cdot (\pi_1 \cdot v + \mathbf{id}_{m_2})$ $[\sim_{\mathcal{R}}]$ T'. By the definition of transitions there exist

$$\begin{array}{l} \langle m', L', R' \rangle \in \mathcal{R} \text{ with } m' \geq m_2 \\ \phi : m' \to m' \text{ a permutation} \\ L'_1 : (m' - m_2) \to 1 \text{ linear and not the identity} \\ u' : 0 \to (m' - m_2) \end{array}$$

such that

$$\begin{aligned} L' &= C \cdot (L'_1 + \mathbf{id}_{m_2}) \cdot \phi \\ s' &= L'_1 \cdot u' \\ T' &= R' \cdot \phi^{-1} \cdot (u' + \mathbf{id}_{m_2}) \end{aligned}$$

and we have

$$\begin{aligned} F \cdot s' &= C \cdot (s' + \pi_2 \cdot v) \\ &= C \cdot (L'_1 \cdot u' + \pi_2 \cdot v) \\ &= C \cdot (L'_1 + \mathbf{id}_{m_2}) \cdot \phi \cdot \phi^{-1} \cdot (u' + \pi_2 \cdot v) \\ &= L' \cdot \phi^{-1} \cdot (u' + \pi_2 \cdot v) \end{aligned}$$

so $s' \xrightarrow{F}_{\mathrm{Cl}(\mathcal{R})} R' \cdot \phi^{-1} \cdot (u' + \pi_2 \cdot v) = T' \cdot \pi_2 \cdot v$. By the definition of [ ] we have $t = R \cdot v = R \cdot (\pi_1 \oplus \pi_2)^{-1} \cdot (\pi_1 \cdot v + \mathbf{id}_{m_2}) \cdot \pi_2 \cdot v \sim_{\mathcal{R}} T' \cdot \pi_2 \cdot v$.

(b) (s is in a component of v) $m \geq 1$ and there exist

$$\begin{array}{l} \pi_1 : m \to 1 \text{ and } \pi_2 : m \to (m-1) \text{ a partition} \\ E : 1 \to 1 \text{ linear} \end{array}$$

such that

$$\begin{aligned} F &= L \cdot (\pi_1 \oplus \pi_2)^{-1} \cdot (E + \pi_2 \cdot v) \\ E \cdot s &= \pi_1 \cdot v \end{aligned}$$

Here $t = R \cdot (\pi_1 \oplus \pi_2)^{-1} \cdot (E + \pi_2 \cdot v) \cdot s$ and $s' \xrightarrow{F}_{\mathrm{Cl}(\mathcal{R})} R \cdot (\pi_1 \oplus \pi_2)^{-1} \cdot (E + \pi_2 \cdot v) \cdot s'$. By Theorem 10 $R \cdot (\pi_1 \oplus \pi_2)^{-1} \cdot (E + \pi_2 \cdot v) \cdot s \sim_{\mathcal{R}} R \cdot (\pi_1 \oplus \pi_2)^{-1} \cdot (E + \pi_2 \cdot v) \cdot s'$.

□

Proof of Theorem 12 First note that if the rewrite rules $\mathcal{R}$ are right-affine then the conclusions of Lemmas 7 and 8 can be strengthened to require H affine. We show that $\mathcal{S} \cup \{ s, s \mid s : 0 \to 1 \}$, where

$$\mathcal{S} \stackrel{\mathit{def}}{=} \{ A \cdot s, A \cdot s' \mid s \approx s' \wedge A : 1 \to 1 \text{ linear} \}$$

is a bisimulation of the form specified. Consider $A : 1 \to 1$ linear and $s \approx s'$. We show that if $A \cdot s \xrightarrow{-} t$ then there exists t' such that $A \cdot s' \xrightarrow{-}{}^{*} t'$ and $t \,\mathcal{S}\, t'$ or $t = t'$. Moreover, if $A \cdot s \xrightarrow{F} T$ for $F \neq \mathbf{id}_1$ then there exists T' such that $A \cdot s' \xrightarrow{-}{}^{*} \xrightarrow{F} T'$ and $T \,[\mathcal{S}]\, T'$ or $T \,[=]\, T'$.

(1) Suppose $A \cdot s \xrightarrow{-} t$. By Lemma 7 one of the following holds:
  (a) There exists some $H : 1 \to 1$ such that $t = H \cdot s$ and for all $\hat{s} : 0 \to 1$ we have $A \cdot \hat{s} \xrightarrow{-} H \cdot \hat{s}$. Moreover, H is affine. It follows that $A \cdot s' \xrightarrow{-} H \cdot s'$. If H is linear then clearly $t = H \cdot s \,\mathcal{S}\, H \cdot s'$, otherwise H does not use its argument so $t = H \cdot s = H \cdot s'$.
  (b) There exist $k \geq 0$, $F : 1 + k \to 1$ linear, $T : k \to 1$, $D : 1 \to 1$ linear and $v : 0 \to k$, such that $s \xrightarrow{F} T$, $A = D \cdot F \cdot (\mathbf{id}_1 + v)$ and $t = D \cdot T \cdot v$.
    (i) Case $F = \mathbf{id}_1$. By $s \approx s'$ there exists T' such that $s' \xrightarrow{-}{}^{*} T' \wedge T \approx T'$. By the definition of reduction $A \cdot s' \xrightarrow{-}{}^{*} A \cdot T'$ and clearly $t = A \cdot T \,\mathcal{S}\, A \cdot T'$.
    (ii) Case $F \neq \mathbf{id}_1$. By $s \approx s'$ there exist s'' and T' such that $s' \xrightarrow{-}{}^{*} s'' \xrightarrow{F} T' \wedge T \approx T'$. By Lemma 9 $F \cdot (s'' + v) \xrightarrow{-} T' \cdot v$. By the definition of reduction $A \cdot s' = D \cdot F \cdot (s' + v) \xrightarrow{-}{}^{*} D \cdot F \cdot (s'' + v) \xrightarrow{-} D \cdot T' \cdot v$, and clearly $t = D \cdot T \cdot v \,\mathcal{S}\, D \cdot T' \cdot v$.

(2) Suppose $A \cdot s \xrightarrow{F} T$ for $F : 1 + n \to 1$ linear and $F \neq \mathbf{id}_1$. By Lemma 8 one of the following holds.
  (a) There exists $H : 1 + n \to 1$ such that $T = H \cdot (s + \mathbf{id}_n)$ and for all $\hat{s} : 0 \to 1$ we have $A \cdot \hat{s} \xrightarrow{F} H \cdot (\hat{s} + \mathbf{id}_n)$. Moreover, H is affine. It follows that $A \cdot s' \xrightarrow{F} H \cdot (s' + \mathbf{id}_n)$. If H is linear in its first argument then $T = H \cdot (s + \mathbf{id}_n) \,[\mathcal{S}]\, H \cdot (s' + \mathbf{id}_n)$, otherwise H does not use its argument so $T = H \cdot (s + \mathbf{id}_n) = H \cdot (s' + \mathbf{id}_n)$ so $T \,[=]\, H \cdot (s' + \mathbf{id}_n)$.
  (b) There exist $p \geq 0$, $E : 1 + p \to 1$ linear, $\hat{T} : p + n \to 1$ and $v : 0 \to p$, such that $s \xrightarrow{F \cdot (E + \mathbf{id}_n)} \hat{T}$, $T = \hat{T} \cdot (v + \mathbf{id}_n)$ and $A = E \cdot (\mathbf{id}_1 + v)$. By $s \approx s'$ there exist s'' and $\hat{T}'$ such that $s' \xrightarrow{-}{}^{*} s'' \xrightarrow{F \cdot (E + \mathbf{id}_n)} \hat{T}' \wedge \hat{T} \,[\approx]\, \hat{T}'$. By the definition of reductions $A \cdot s' \xrightarrow{-}{}^{*} A \cdot s''$. By Lemma 9 $A \cdot s'' = E \cdot (s'' + v) \xrightarrow{F} \hat{T}' \cdot (v + \mathbf{id}_n)$. Clearly $T = \hat{T} \cdot (v + \mathbf{id}_n) \,[\mathcal{S}]\, \hat{T}' \cdot (v + \mathbf{id}_n)$.

□

C Proofs for Section 4

This appendix contains the lemmas required for the main congruence result of Section 4. It is divided into three subsections, of dissection, forwards, and backwards lemmas respectively. Only Lemma 27 of §C.2, showing that if $A \cdot s \longrightarrow t$ then s has a suitable labelled transition, is proved in detail; other proofs can be found in the technical report version.

This subsection contains the statements of lemmas required for the proof of the main dissection lemma (Lemma 13), together with the statements of some auxiliary simple dissection results used elsewhere.

Lemma 17 *If $B : m \to 1$ linear then there exist m_1, m_3, $\pi_1 : m \to m_1$ and $\pi_3 : m \to m_3$ a partition, and $B' : m_1 \to 1$ linear and deep, such that $m = m_1 + m_3$ and $B \equiv \mathbf{par}_{1+m_3} \cdot (B' + \mathbf{id}_{m_3}) \cdot (\pi_1 \oplus \pi_3)$.*

Lemma 18 *If $C : 1 + m \to 1$ linear then there exist m_1, m_2, $\pi_1 : m \to m_1$ and $\pi_2 : m \to m_2$ a partition, and $C' : (1+m_2) \to 1$ linear and 1-separated, such that $m = m_1 + m_2$ and $C \equiv C' \cdot (\mathbf{par}_{1+m_1} + \mathbf{id}_{m_2}) \cdot (\mathbf{id}_1 + \pi_1 \oplus \pi_2)$.*

Lemma 19 *If $B : m \to 1$ is linear for $m \geq 0$ then there exist $n \in 1..m$, $\hat{m}_i \geq 1$ for $i \in 1..n$ summing to m, $\theta_i : m \to \hat{m}_i$ for $i \in 1..n$ a partition, $B_i : \hat{m}_i \to 1$ for $i \in 1..n$ linear and shallow, and $B' : n \to 1$ linear and clean, such that $B \equiv B' \cdot (B_1 + \ldots + B_n) \cdot (\theta_1 \oplus \ldots \oplus \theta_n)$.*

Lemma 20 *If $m \geq 0$, $B : m \to 1$ is linear and clean, $b : 0 \to m$, and $B \cdot b \equiv c$, then there exist $B' : m \to 1$ linear and $b' : 0 \to m$ such that $B \equiv B'$, $b \equiv b'$ and $c = B' \cdot b'$.*

Lemma 21 *If $m \geq 0$,*

$$\begin{array}{ll} A : 1 \to 1 & B : m \to 1 \\ a : 0 \to 1 & b : 0 \to m \end{array}$$

with A and B linear, and $A \cdot a = B \cdot b$, then one of the clauses of the conclusion of Lemma 13 holds.

Proof By Lemmas 6, 18 and 17. □

Proof of Lemma 13 The proof is by induction on the derivations of structural congruence, showing that if $A \cdot a \equiv B \cdot b$ or $B \cdot b \equiv A \cdot a$ then one of the clauses of the conclusion holds. The degenerate cases $m = 0$, $A = \mathbf{id}_1$ and $B = \mathbf{id}_1$ are dealt with separately. □

Lemma 22 *If*

$$\begin{array}{ll} A : 1 \to 1 & B : 1 \to 1 \\ a : 0 \to 1 & b : 0 \to 1 \end{array}$$

with A and B linear, and $A \cdot a \equiv B \cdot b$, then one of the following holds.

(1) (a and b are disjoint) There exists $E : 2 \to 1$ linear such that $A \equiv E \cdot (\_ + b)$ and $B \equiv E \cdot (a + \_)$.

(2) *(a and b overlap) There exist* $C : 1 \to 1$ *linear and* $z_{\mathsf{A,b}}$, $z_{\mathsf{a,B}}$ *and* $z_{\mathsf{a,b}}$ *such that*

$$\begin{array}{ll} A \equiv C \cdot (z_{\mathsf{A,b}} \mid \_) & a \equiv z_{\mathsf{a,B}} \mid z_{\mathsf{a,b}} \\ B \equiv C \cdot (z_{\mathsf{a,B}} \mid \_) & b \equiv z_{\mathsf{A,b}} \mid z_{\mathsf{a,b}} \end{array}$$

and moreover $z_{\mathsf{a,b}} \not\equiv 0$

(3) *(A is properly in B and b is deeply in a) There exists* $D : 1 \to 1$ *linear and deep such that* $a \equiv D \cdot b$ *and* $A \cdot D \equiv B$.

(4) *(B is properly in A and a is deeply in b) There exists* $D : 1 \to 1$ *linear and deep such that* $D \cdot a \equiv b$ *and* $A \equiv B \cdot D$.

Lemma 23 *If* $m \geq 0$,

$$\begin{array}{ll} a_1 : 0 \to 1 & C : m \to 1 \\ a_2 : 0 \to 1 & d : 0 \to m \end{array}$$

with C *linear, and* $a_1 \mid a_2 \equiv C \cdot d$, *then there exist*

$$\begin{array}{l} m_1, m_2 \text{ and } m_3 \text{ such that } m_1 + m_2 + m_3 = m \\ \pi_i : m \to m_i \text{ for } i \in \{1,2,3\} \text{ a partition} \\ C_1 : m_1 \to 1 \text{ linear and deep} \\ C_2 : m_2 \to 1 \text{ linear and deep} \\ e_1 : 0 \to m_3 \\ e_2 : 0 \to m_3 \end{array}$$

such that

$$\begin{array}{rl} a_1 \equiv & \mathbf{par}_{1+m_3} \cdot (C_1 \cdot \pi_1 \cdot d + e_1) \\ a_2 \equiv & \mathbf{par}_{1+m_3} \cdot (C_2 \cdot \pi_2 \cdot d + e_2) \\ C \equiv & \mathbf{par}_{2+m_3} \cdot (C_1 + C_2 + \mathbf{id}_{m_3}) \cdot (\pi_1 \oplus \pi_2 \oplus \pi_3) \\ \pi_3 \cdot d \equiv & \mathbf{ppar}_{m_3} \cdot (e_1 + e_2) \end{array}$$

There are m_1 *of the* d *in* a_1, m_2 *of the* d *in* a_2 *and* m_3 *of the* d *potentially overlapping* a_1 *and* a_2. *The latter are split into* e_1, *in* a_1, *and* e_2, *in* a_2.

Lemma 24 *If* $m \geq 0$,

$$\begin{array}{ll} a_1 : 0 \to 1 & C : m \to 1 \\ a_2 : 0 \to 1 & d : 0 \to m \end{array}$$

with C *linear and deep, and* $a_1 \mid a_2 \equiv C \cdot d$, *then there exist*

$$\begin{array}{l} m_1 \text{ and } m_2 \text{ such that } m_1 + m_2 = m \\ \pi_i : m \to m_i \text{ for } i \in \{1,2\} \text{ a partition} \\ C_1 : m_1 \to 1 \text{ linear and deep} \\ C_2 : m_2 \to 1 \text{ linear and deep} \end{array}$$

such that

$$\begin{aligned} a_1 &\equiv C_1 \cdot \pi_1 \cdot d \\ a_2 &\equiv C_2 \cdot \pi_2 \cdot d \\ C &\equiv \mathbf{par}_2 \cdot (C_1 + C_2) \cdot (\pi_1 \oplus \pi_2) \end{aligned}$$

There are m_1 of the d in a_1 and m_2 of the d in a_2.

Lemma 25 *If $m \geq 1$,*

$$\begin{aligned} &A : 1 \to 1 \qquad b : 0 \to m \\ &s : 0 \to 1 \end{aligned}$$

with A linear and deep, and $A \cdot s \equiv \mathbf{par}_m \cdot b$, then there exist

$$\begin{aligned} &\pi_1 : m \to 1 \text{ and } \pi_2 : m \to (m-1) \text{ a partition} \\ &\hat{A} : 1 \to 1 \text{ linear and deep} \\ &\hat{a} : 0 \to (m-1) \end{aligned}$$

such that

$$\begin{aligned} A &\equiv \mathbf{par}_m \cdot (\hat{A} + \hat{a}) \\ \hat{A} \cdot s + \hat{a} &\equiv (\pi_1 \oplus \pi_2) \cdot b \end{aligned}$$

Lemma 26 *If $m \geq 1$,*

$$\begin{aligned} &A : 1 \to 1 \qquad b : 0 \to m \\ &s : 0 \to 1 \end{aligned}$$

with A linear and shallow, and $A \cdot s \equiv \mathbf{par}_m \cdot b$, then there exist

$$\begin{aligned} &\hat{a} : 0 \to m \\ &\hat{s} : 0 \to m \end{aligned}$$

such that

$$\begin{aligned} A &\equiv \mathbf{par}_{1+m} \cdot (\mathbf{id}_1 + \hat{a}) \\ s &\equiv \mathbf{par}_m \cdot \hat{s} \\ \mathbf{ppar}_m \cdot (\hat{a} + \hat{s}) &\equiv b \end{aligned}$$

C.2 Forwards Lemmas

The three lemmas in this subsection show that if $A \cdot s$ has some labelled transition, where $A : 1 \to 1$ is linear, then either the transition is independent of s or s has a related labelled transition. We have chosen to consider arbitrary A – one could instead restrict to *atomic* A, in which the hole is under exactly one symbol. It is not clear whether this would allow significant simplifications.

Lemma 27 *If* $A \cdot s \xrightarrow{I} t$ *for* $A : 1 \to 1$ *linear and* $I \equiv \mathbf{id}_1$ *then one of the following holds.*

(1) There exists some $H : 1 \to 1$ *such that* $t \equiv H \cdot s$ *and* $\forall \hat{s} : 0 \to 1 \,.\; A \cdot \hat{s} \xrightarrow{-} H \cdot \hat{s}$.
(2) There exist

$$\begin{array}{l} n \geq 0 \\ F : (1+n) \to 1 \textit{ linear} \\ T : n \to 1 \\ C \in \mathcal{C} \\ v : 0 \to n \end{array}$$

such that $s \xrightarrow{F} T$, $A \equiv C \cdot F \cdot (\mathbf{id}_1 + v)$ *and* $t \equiv C \cdot T \cdot v$.

Proof By the definition of labelled transitions

$$\exists \langle m, L, R \rangle \in \mathcal{R}, B \in \mathcal{C}, u : 0 \to m \,.\; A \cdot s \equiv B \cdot L \cdot u \wedge B \cdot R \cdot u \equiv t$$

The proof involves a number of cases, summarized below.

1 s and $L \cdot u$ are disjoint. Clause 1 holds.
2 s and $L \cdot u$ may overlap.
  a the overlap is trivial. Clause 1 holds.
  b the overlap is non-trivial. Clause 2 holds with F shallow in 1 and not $\mathbf{id}_1$.
3 $L \cdot u$ is deeply in s. Clause 2 holds with $F = \mathbf{id}_1$.
4 s is deeply in $L \cdot u$.
  a s is not deeply in any component of u.
    i s non-trivially overlaps L. Clause 2 holds with F deep in 1.
    ii s does not overlap L. Clause 1 holds.
  b s is deeply in a component of u. Clause 1 holds.

We now consider the cases in detail. Each case involves verification of the existence of a labelled transition and of other equational conditions. The existential witness for a labelled transition is generally given explicitly; the statements of the required equational conditions are often elided (but can be found in the technical report version). Applying Lemma 22 to $A \cdot s \equiv B \cdot (L \cdot u)$ we have

(1) (s and $L \cdot u$ are disjoint) There exists $E : 2 \to 1$ linear such that

$$A \equiv E \cdot (\_ + L \cdot u) \qquad B \equiv E \cdot (s + \_)$$

Putting $H = E \cdot (\_ + R \cdot u)$ we have clause 1 of the conclusion.

(2) (s and $L \cdot u$ overlap) There exist $D : 1 \to 1$ linear and $z_{\mathsf{A},\mathsf{L} \cdot \mathsf{u}}$, $z_{\mathsf{s},\mathsf{B}}$ and $z_{\mathsf{s},\mathsf{L} \cdot \mathsf{u}}$ such that

$$\begin{aligned} A &\equiv D\cdot(z_{\mathsf{A,L\cdot u}} \mid \_) \\ B &\equiv D\cdot(z_{\mathsf{s,B}} \mid \_) \\ s &\equiv z_{\mathsf{s,B}} \mid z_{\mathsf{s,L\cdot u}} \\ L\cdot u &\equiv z_{\mathsf{A,L\cdot u}} \mid z_{\mathsf{s,L\cdot u}} \end{aligned}$$

and moreover $z_{\mathsf{s,L\cdot u}} \not\equiv 0$ Applying Lemma 23 to $z_{\mathsf{s,L\cdot u}} \mid z_{\mathsf{A,L\cdot u}} \equiv L\cdot u$ we have that there exist

m_1, m_2 and m_3 such that $m_1 + m_2 + m_3 = m$
$\pi_i : m \to m_i$ for $i \in \{1,2,3\}$ a partition
$L_1 : m_1 \to 1$ linear and deep
$L_2 : m_2 \to 1$ linear and deep
$e_1 : 0 \to m_3$
$e_2 : 0 \to m_3$

such that

$$\begin{aligned} z_{\mathsf{s,L\cdot u}} &\equiv \mathbf{par}_{1+m_3}\cdot(L_1\cdot\pi_1\cdot u + e_1) \\ z_{\mathsf{A,L\cdot u}} &\equiv \mathbf{par}_{1+m_3}\cdot(L_2\cdot\pi_2\cdot u + e_2) \\ L &\equiv \mathbf{par}_{2+m_3}\cdot(L_1 + L_2 + \mathbf{id}_{m_3})\cdot(\pi_1 \oplus \pi_2 \oplus \pi_3) \\ \pi_3\cdot u &\equiv \mathbf{ppar}_{m_3}\cdot(e_1 + e_2) \end{aligned}$$

There are m_1 of the u in $z_{\mathsf{s,L\cdot u}}$, m_2 of the u in $z_{\mathsf{A,L\cdot u}}$ and m_3 of the u potentially overlapping $z_{\mathsf{s,L\cdot u}}$ and $z_{\mathsf{A,L\cdot u}}$. The latter are split into e_1, in $z_{\mathsf{s,L\cdot u}}$, and e_2, in $z_{\mathsf{A,L\cdot u}}$.

Note that as L_2 deep we have $L_2\cdot\pi_2\cdot u \equiv 0 \iff m_2 = 0 \wedge L_2 \equiv \langle 0\rangle_0$. We now have two cases, one with $L\cdot u$ properly in s and one with a non-trivial overlap.

(a) Case $L_2\cdot\pi_2\cdot u \equiv 0 \wedge m_3 = 0$. Here $m_2 = m_3 = 0$, $L_2 \equiv \langle 0\rangle_0$, $L \equiv L_1\cdot\pi_1$ and $z_{\mathsf{A,L\cdot u}} \equiv 0$ so $s \equiv z_{\mathsf{s,B}} \mid L\cdot u$. Taking

$$\begin{aligned} n &= 0 \\ F &= \mathbf{id}_1 && : 1 \to 1 \\ T &= (z_{\mathsf{s,B}} \mid \_)\cdot R\cdot u && : 0 \to 1 \\ C &= A && : 1 \to 1 \\ v &= \langle\rangle_0 && : 0 \to 0 \end{aligned}$$

we have clause 2 of the conclusion.

(b) Case $L_2\cdot\pi_2\cdot u \not\equiv 0 \vee m_3 \neq 0$. Taking

$$\begin{aligned} n &= m_3 + m_2 \\ F &= \mathbf{par}_{2+m_3}\cdot(\mathbf{id}_1 + \mathbf{id}_{m_3} + L_2) \\ T &= (\_ \mid z_{\mathsf{s,B}})\cdot R\cdot(\pi_1 \oplus \pi_3 \oplus \pi_2)^{-1} \\ &\qquad \cdot(\pi_1\cdot u + \mathbf{ppar}_{m_3}\cdot(\mathbf{id}_{m_3} + e_1) + \mathbf{id}_{m_2}) \\ C &= D \\ v &= (e_2 + \pi_2\cdot u) \end{aligned}$$

we have clause 2 of the conclusion. There is a transition

$s \overset{\mathbf{par}_{2+m_3} \cdot (\mathbf{id}_1 + \mathbf{id}_{m_3} + L_2)}{\longrightarrow} (\_ \mid z_{\mathsf{s,B}}) \cdot R \cdot (\pi_1 \oplus \pi_3 \oplus \pi_2)^{-1} \cdot (\pi_1 \cdot u + \mathbf{ppar}_{m_3} \cdot (\mathbf{id}_{m_3} + e_1) + \mathbf{id}_{m_2})$

with witness

$\langle m, L, R \rangle \in \mathcal{R}$

m_1, m_2 and m_3 such that $m_1 + m_2 + m_3 = m$

$(\pi_1 \oplus \pi_3 \oplus \pi_2) : m \to m$ a permutation

$\mathbf{par}_{2+m_3} \cdot (\mathbf{id}_1 + \mathbf{id}_{m_3} + L_2) : 1 + m_3 + m_2 \to 1$ linear, shallow in argument 1, and not $\mathbf{id}_1$

$z_{\mathsf{s,B}} : 0 \to 1$

$L_1 : m_1 \to 1$ linear and deep

$L_2 : m_2 \to 1$ linear and deep

$(\pi_1 \cdot u) : 0 \to m_1$

$e_1 : 0 \to m_3$

If $m_3 = 0$ then by assumption $L_2 \cdot \pi_2 \cdot u \not\equiv 0$, hence $L_2 \not\equiv \langle 0 \rangle_0$ so $F \not\equiv \mathbf{id}_1$. Further, $z_{\mathsf{s,L \cdot u}} \equiv L_1 \cdot \pi_1 \cdot u$ so we have $L_1 \cdot \pi_1 \cdot u \not\equiv 0$, hence $L_1 \not\equiv \langle 0 \rangle_0$.

(3) (A is properly in B and $L \cdot u$ is deeply in s) There exists $D : 1 \to 1$ linear and deep such that

$$s \equiv D \cdot L \cdot u$$
$$A \cdot D \equiv B$$

Taking

$$\begin{aligned} n &= 0 \\ F &= \mathbf{id}_1 & &: 1 \to 1 \\ T &= D \cdot R \cdot u & &: 0 \to 1 \\ C &= A & &: 1 \to 1 \\ v &= \langle\rangle_0 & &: 0 \to 0 \end{aligned}$$

we have clause 2 of the conclusion.

(4) (B is properly in A and s is deeply in $L \cdot u$) There exists $D : 1 \to 1$ linear and deep such that

$$D \cdot s \equiv L \cdot u$$
$$A \equiv B \cdot D$$

Applying Lemma 13 to $D \cdot s \equiv L \cdot u$ we have one of the following

(a) (s is not deeply in any component of u) There exist

m_1, m_2 and m_3 such that $m_1 + m_2 + m_3 = m$

$\pi_1 : m \to m_1$, $\pi_2 : m \to m_2$ and $\pi_3 : m \to m_3$ a partition

$L_2 : 1 + m_2 \to 1$ linear and 1-separated

$L_1 : m_1 \to 1$ linear and deep

$e_1 : 0 \to m_3$

$e_2 : 0 \to m_3$

such that

$$\begin{aligned} D &\equiv L_2 \cdot(\mathbf{par}_{1+m_3} \cdot(\mathbf{id}_1 + e_2) + \pi_2 \cdot u) \\ s &\equiv \mathbf{par}_{1+m_3} \cdot(L_1 \cdot \pi_1 \cdot u + e_1) \\ L &\equiv L_2 \cdot(\mathbf{par}_{1+m_3} \cdot(L_1 + \mathbf{id}_{m_3}) + \mathbf{id}_{m_2}) \cdot(\pi_1 \oplus \pi_3 \oplus \pi_2) \\ \pi_3 \cdot u &\equiv \mathbf{ppar}_{m_3} \cdot(e_1 + e_2) \end{aligned}$$

There are m_1 of the u in s, m_2 of the u in D and m_3 of the u potentially overlapping D and s. The latter are split into e_1, in s, and e_2, in D.

(i) Case $m_3 = 1 \implies L_1 \not\equiv \langle 0\rangle_0$. Since D is deep we know that L_2 is deep in argument 1. Taking

$$\begin{aligned} n &= m_3 + m_2 \\ F &= L_2 \cdot(\mathbf{par}_{1+m_3} + \mathbf{id}_{m_2}) \\ T &= R \cdot(\pi_1 \oplus \pi_3 \oplus \pi_2)^{-1} \cdot(\pi_1 \cdot u + \mathbf{ppar}_{m_3} \cdot(\mathbf{id}_{m_3} + e_1) + \mathbf{id}_{m_2}) \\ C &= B \\ v &= (e_2 + \pi_2 \cdot u) \end{aligned}$$

we have clause 2 of the conclusion. There is a transition
$s \stackrel{L_2 \cdot(\mathbf{par}_{1+m_3} + \mathbf{id}_{m_2})}{\longrightarrow} R \cdot(\pi_1 \oplus \pi_3 \oplus \pi_2)^{-1} \cdot(\pi_1 \cdot u + \mathbf{ppar}_{m_3} \cdot(\mathbf{id}_{m_3} + e_1) + \mathbf{id}_{m_2})$
with witness
$\langle m, L, R\rangle \in \mathcal{R}$
m_1, m_2 and m_3 such that $m_1 + m_2 + m_3 = m$
$(\pi_1 \oplus \pi_3 \oplus \pi_2) : m \to m$ a permutation
$L_2 \cdot(\mathbf{par}_{1+m_3} + \mathbf{id}_{m_2}) : 1 + m_3 + m_2 \to 1$ linear, deep in argument 1
$L_1 : m_1 \to 1$ linear and deep
$L_2 : 1 + m_2 \to 1$ linear, deep in argument 1 and 1-separated
$\pi_1 \cdot u : 0 \to m_1$
$e_1 : 0 \to m_3$

(ii) Case $m_3 = 1 \wedge L_1 \equiv \langle 0\rangle_0$. Putting

$$H = B \cdot R \cdot(\pi_1 \oplus \pi_3 \oplus \pi_2)^{-1} \cdot(\mathbf{par}_2 \cdot(\mathbf{id}_1 + e_2) + \pi_2 \cdot u)$$

we have clause 1 of the conclusion.

(b) (s is deeply in a component of u) $m \geq 1$ and there exist

$\pi_1 : m \to 1$ and $\pi_2 : m \to (m-1)$ a partition
$E : 1 \to 1$ linear and deep

such that

$$\begin{aligned} D &\equiv L \cdot(\pi_1 \oplus \pi_2)^{-1} \cdot(E + \pi_2 \cdot u) \\ E \cdot s &\equiv \pi_1 \cdot u \end{aligned}$$

Putting $H = B \cdot R \cdot (\pi_1 \oplus \pi_2)^{-1} \cdot (E + \pi_2 \cdot u)$ we have clause 1 of the conclusion.

□

Lemma 28 *If $A \cdot s \xrightarrow{F} T$ for $A : 1 \to 1$ linear and $F : 1 + n \to 1$ linear and deep in 1 then one of the following holds.*

(1) *There exists $H : 1 + n \to 1$ such that $T \equiv H \cdot (s + \mathbf{id}_n)$ and for all $\hat{s} : 0 \to 1$ we have $A \cdot \hat{s} \xrightarrow{F} H \cdot (\hat{s} + \mathbf{id}_n)$.*

(2) *There exist*

$$
\begin{aligned}
&m_{13} \geq 0 \text{ and } m_{12} \geq 0 \text{ and } m_2 \geq 0 \text{ and } m_3 \geq 0 \\
&\qquad \text{such that } n = m_3 + m_2 \\
&L_{12} : 1 + m_{12} \to 1 \text{ linear, deep in } 1 \text{ and } 1\text{-separated} \\
&L_2 : 1 + m_2 \to 1 \text{ linear, deep in argument } 1 \text{ and } 1\text{-separated} \\
&\hat{T} : m_{13} + m_{12} + m_3 + m_2 \to 1 \\
&v_3 : 0 \to m_{13} \\
&v_2 : 0 \to m_{12} \\
&e : 0 \to m_3
\end{aligned}
$$

such that

$$
\begin{aligned}
&s \xrightarrow{L_2 \cdot (\mathbf{par}_{1+m_3} + \mathbf{id}_{m_2}) \cdot (L_{12} + \mathbf{id}_n) \cdot (\mathbf{par}_{1+m_{13}} + \mathbf{id}_{m_{12}+m_3+m_2})} \hat{T} \\
&F \equiv L_2 \cdot (\mathbf{par}_{1+m_3} + \mathbf{id}_{m_2}) \\
&T \equiv \hat{T} \cdot (v_3 + v_2 + \mathbf{ppar}_{m_3} \cdot (e + \mathbf{id}_{m_3}) + \mathbf{id}_{m_2}) \\
&A \equiv \mathbf{par}_{1+m_3} \cdot (L_{12} \cdot (\mathbf{par}_{1+m_{13}} \cdot (\mathbf{id}_1 + v_3) + v_2) + e)
\end{aligned}
$$

(3) *There exist*

$$
\begin{aligned}
&m_{12} \geq 0 \text{ and } m_2 \geq 0 \text{ and } m_3 \geq 0 \text{ such that } n = m_3 + m_2 \\
&L_{12} : m_{12} \to 1 \text{ linear and deep} \\
&L_2 : 1 + m_2 \to 1 \text{ linear, deep in argument } 1 \text{ and } 1\text{-separated} \\
&\hat{T} : m_3 + m_{12} + m_2 \to 1 \\
&v : 0 \to m_{12} \\
&\hat{\hat{a}} : 0 \to m_3
\end{aligned}
$$

such that

$$
\begin{aligned}
&s \xrightarrow{L_2 \cdot (\mathbf{par}_{2+m_3} + \mathbf{id}_{m_2}) \cdot (\mathbf{id}_1 + \mathbf{id}_{m_3} + L_{12} + \mathbf{id}_{m_2})} \hat{T} \\
&F \equiv L_2 \cdot (\mathbf{par}_{1+m_3} + \mathbf{id}_{m_2}) \\
&T \equiv \hat{T} \cdot (\mathbf{ppar}_{m_3} \cdot (\mathbf{id}_{m_3} + \hat{\hat{a}}) + v + \mathbf{id}_{m_2}) \\
&A \equiv \mathbf{par}_{2+m_3} \cdot (\mathbf{id}_1 + L_{12} \cdot v + \hat{\hat{a}})
\end{aligned}
$$

Proof By the definition of transitions there exist

$\langle m, L, R\rangle \in \mathcal{R}$
m_1, m_2 and m_3 such that $m_1 + m_2 + m_3 = m$ and $n = m_3 + m_2$
$\pi : m \to m$ a permutation
$L_1 : m_1 \to 1$ linear and deep
$L_2 : 1 + m_2 \to 1$ linear, deep in argument 1 and 1-separated
$u : 0 \to m_1$
$e : 0 \to m_3$

such that

$$
\begin{aligned}
&L \equiv L_2 \cdot (\mathbf{par}_{1+m_3} \cdot (L_1 + \mathbf{id}_{m_3}) + \mathbf{id}_{m_2}) \cdot \pi \\
&A \cdot s \equiv \mathbf{par}_{1+m_3} \cdot (L_1 \cdot u + e) \\
&T \equiv R \cdot \pi^{-1} \cdot (u + \mathbf{ppar}_{m_3} \cdot (\mathbf{id}_{m_3} + e) + \mathbf{id}_{m_2}) \\
&F \equiv L_2 \cdot (\mathbf{par}_{1+m_3} + \mathbf{id}_{m_2}) \\
&m_3 = 1 \implies L_1 \not\equiv \langle 0\rangle_0
\end{aligned}
$$

The proof involves a number of cases, summarized below.

1 A deep.
 a s is not in e.
  i s is not deeply in any component of u.
   A s and L have a non-trivial overlap. Clause 2 holds.
   B s is in u. Clause 1 holds.
  ii s is deeply in a component of u. Clause 1 holds.
 b s is in one component of e. Clause 1 holds.
2 A shallow.
 a s and L have a non-trivial overlap. Clause 3 holds.
 b s is in e. Clause 1 holds.

□

Lemma 29 *If $A \cdot s \xrightarrow{F} T$ for $A : 1 \to 1$ linear and $F : 1 + n \to 1$ linear, shallow in 1 and $F \not\equiv \mathbf{id}_1$ then one of the following holds.*

(1) There exists $H : 1 + n \to 1$ such that $T \equiv H \cdot (s + \mathbf{id}_n)$ and for all $\hat{s} : 0 \to 1$ we have $A \cdot \hat{s} \xrightarrow{F} H \cdot (\hat{s} + \mathbf{id}_n)$.

(2) There exist

$$\begin{array}{l} m_{13} \geq 0 \textit{ and } m_{12} \geq 0 \textit{ and } m_2 \geq 0 \textit{ and } m_3 \geq 0 \\ \qquad \textit{such that } n = m_3 + m_2 \\ q : 0 \to 1 \\ L_{12} : 1 + m_{12} \to 1 \textit{ linear, deep and } 1\textit{-separated} \\ L_2 : m_2 \to 1 \quad \textit{linear and deep} \\ \hat{T} : m_{13} + m_{12} + m_3 + m_2 \to 1 \\ v_3 : 0 \to m_{13} \\ v_2 : 0 \to m_{12} \\ e : 0 \to m_3 \end{array}$$

such that

$$\begin{array}{l} s \overset{\mathbf{par}_{2+m_3} \cdot (L_{12} + \mathbf{id}_{m_3} + L_2) \cdot (\mathbf{par}_{1+m_{13}} + \mathbf{id}_{m_{12}+m_3+m_2})}{\longrightarrow} \hat{T} \\ F \equiv \mathbf{par}_{2+m_3} \cdot (\mathbf{id}_1 + \mathbf{id}_{m_3} + L_2) \\ T \equiv \mathbf{par}_2 \cdot (q + \hat{T} \cdot (v_3 + v_2 + \mathbf{ppar}_{m_3} \cdot (e + \mathbf{id}_{m_3}) + \mathbf{id}_{m_2})) \\ A \equiv \mathbf{par}_{2+m_3} \cdot (q + L_{12} \cdot (\mathbf{par}_{1+m_{13}} \cdot (\mathbf{id}_1 + v_3) + v_2) + e) \\ m_3 = 0 \implies L_2 \not\equiv \langle 0 \rangle_0 \end{array}$$

(3) There exist

$$\begin{array}{l} m_{12} \geq 0 \textit{ and } m_2 \geq 0 \textit{ and } m_3 \geq 0 \textit{ such that } n = m_3 + m_2 \\ a' : 0 \to 1 \\ L_{12} : m_{12} \to 1 \textit{ linear and deep} \\ L_2 : m_2 \to 1 \quad \textit{linear and deep} \\ \hat{T} : m_3 + m_{12} + m_2 \to 1 \\ v_2 : 0 \to m_{12} \\ a''' : 0 \to m_3 \end{array}$$

such that

$$\begin{array}{l} s \overset{\mathbf{par}_{3+m_3} \cdot (\mathbf{id}_1 + \mathbf{id}_{m_3} + L_{12} + L_2)}{\longrightarrow} \hat{T} \\ F \equiv \mathbf{par}_{2+m_3} \cdot (\mathbf{id}_1 + \mathbf{id}_{m_3} + L_2) \\ T \equiv \mathbf{par}_2 \cdot (a' + \hat{T} \cdot (\mathbf{ppar}_{m_3} \cdot (\mathbf{id}_{m_3} + a''') + v_2 + \mathbf{id}_{m_2})) \\ A \equiv \mathbf{par}_{1+2+m_3} \cdot (\mathbf{id}_1 + a' + L_{12} \cdot v_2 + a''') \\ m_3 = 0 \implies L_2 \not\equiv \langle 0 \rangle_0 \end{array}$$

Proof By the definition of transitions there exist

$\langle m, L, R\rangle \in \mathcal{R}$
m_1, m_2 and m_3 such that $m_1 + m_2 + m_3 = m$ and $n = m_3 + m_2$
$\pi : m \to m$ a permutation
$q : 0 \to 1$
$L_1 : m_1 \to 1$ linear and deep
$L_2 : m_2 \to 1$ linear and deep
$u : 0 \to m_1$
$e : 0 \to m_3$

such that

$$
\begin{aligned}
&L \equiv \mathbf{par}_{2+m_3} \cdot (L_1 + \mathbf{id}_{m_3} + L_2) \cdot \pi \\
&A \cdot s \equiv \mathbf{par}_{2+m_3} \cdot (q + L_1 \cdot u + e) \\
&T \equiv \mathbf{par}_2 \cdot (q + R \cdot \pi^{-1} \cdot (u + \mathbf{ppar}_{m_3} \cdot (\mathbf{id}_{m_3} + e) + \mathbf{id}_{m_2})) \\
&F \equiv \mathbf{par}_{2+m_3} \cdot (\mathbf{id}_1 + \mathbf{id}_{m_3} + L_2) \\
&m_3 = 0 \implies L_1 \not\equiv \langle 0\rangle_0
\end{aligned}
$$

By $F \not\equiv \mathbf{id}_1$ we also have $m_3 = 0 \implies L_2 \not\equiv \langle 0\rangle_0$. The proof involves a number of cases, summarized below.

1 A deep.
- **a** s is in q. Clause 1 holds.
- **b** s is in $L_1 \cdot u$.
  - **i** s is not deeply in any component of u.
    - **A** s and L have a non-trivial overlap. Clause 2 holds.
    - **B** s is in u. Clause 1 holds.
  - **ii** s is deeply in a component of u. Clause 1 holds.
- **c** s is in e. Clause 1 holds.

2 A shallow.
- **a** s and L have a non-trivial overlap. Clause 3 holds.
- **b** s is in q. Clause 1 holds.

□

C.3 Backwards Lemmas

The five lemmas in this subsection are approximate converses to those in Section C.2. The first shows that if $s \xrightarrow{F} T$ then $F \cdot (s + v)$ has a reduction to $T \cdot v$. The other four show that if $s \xrightarrow{F \cdot G} T$ then s, in a context constructed from G, has a transition with label F. This is done for F and G deep and shallow in their first arguments.

Lemma 30 *If* $s \xrightarrow{F} T$ *for* $F : 1 + n \to 1$ *then for all* $v : 0 \to n$ *we have* $F \cdot (s + v) \xrightarrow{-} T \cdot v$.

Proof Straightforward case analysis on the three possible forms of F. □

Lemma 31 *If* $s \xrightarrow{\hat{L}_2 \cdot (\mathbf{par}_{1+m_3} + \mathbf{id}_{m_2}) \cdot (L_{12} + \mathbf{id}_{m_3+m_2}) \cdot (\mathbf{par}_{1+m_{13}} + \mathbf{id}_{m_{12}+m_3+m_2})} \hat{T}$, *where*

$$\begin{array}{l} m_{13} \geq 0 \textit{ and } m_{12} \geq 0 \textit{ and } m_2 \geq 0 \textit{ and } m_3 \geq 0 \\ \hat{L}_2 : 1 + m_2 \to 1 \textit{ linear, deep in } 1 \textit{ and } 1\textit{-separated} \\ L_{12} : 1 + m_{12} \to 1 \textit{ linear, deep and } 1\textit{-separated} \\ \hat{T} : m_{13} + m_{12} + m_3 + m_2 \to 1 \end{array}$$

then for all $v_3 : 0 \to m_{13}$, $v_2 : 0 \to m_{12}$, *and* $e : 0 \to m_3$ *we have*

$$\begin{array}{rl} & \mathbf{par}_{1+m_3} \cdot (L_{12} \cdot (\mathbf{par}_{1+m_{13}} \cdot (s + v_3) + v_2) + e) \\ \xrightarrow{\hat{L}_2 \cdot (\mathbf{par}_{1+m_3} + \mathbf{id}_{m_2})} & \hat{T} \cdot (v_3 + v_2 + \mathbf{ppar}_{m_3} \cdot (e + \mathbf{id}_{m_3}) + \mathbf{id}_{m_2}) \end{array}$$

Proof By the definition of deep labelled transitions, using the fact that L_{12} is deep in 1 and 1-separated to justify some cancellation steps. □

Lemma 32 *If* $s \xrightarrow{L_2 \cdot (\mathbf{par}_{2+m_3} + \mathbf{id}_{m_2}) \cdot (\mathbf{id}_1 + \mathbf{id}_{m_3} + L_{12} + \mathbf{id}_{m_2})} \hat{T}$, *where*

$$\begin{array}{l} m_{12} \geq 0 \textit{ and } m_2 \geq 0 \textit{ and } m_3 \geq 0 \\ L_{12} : m_{12} \to 1 \textit{ linear and deep} \\ L_2 : 1 + m_2 \to 1 \textit{ linear, deep in argument } 1 \textit{ and } 1\textit{-separated} \\ \hat{T} : m_3 + m_{12} + m_2 \to 1 \end{array}$$

then for all $v : 0 \to m_{12}$ *and* $\hat{\hat{a}} : 0 \to m_3$ *we have*

$$\begin{array}{rl} & \mathbf{par}_{2+m_3} \cdot (\mathbf{id}_1 + L_{12} \cdot v + \hat{\hat{a}}) \cdot s \\ \xrightarrow{L_2 \cdot (\mathbf{par}_{1+m_3} + \mathbf{id}_{m_2})} & \hat{T} \cdot (\mathbf{ppar}_{m_3} \cdot (\mathbf{id}_{m_3} + \hat{\hat{a}}) + v + \mathbf{id}_{m_2}) \end{array}$$

Proof By the definition of deep labelled transitions, using the fact that L_2 is deep in 1 and 1-separated, and L_{12} is deep, to justify some cancellation steps. □

Lemma 33 *If* $s \xrightarrow{\mathbf{par}_{2+m_3} \cdot (L_{12} + \mathbf{id}_{m_3} + L_2) \cdot (\mathbf{par}_{1+m_{13}} + \mathbf{id}_{m_{12}+m_3+m_2})} \hat{T}$, *where*

$$\begin{array}{l} m_{12} \geq 0 \textit{ and } m_{13} \geq 0 \textit{ and } m_2 \geq 0 \textit{ and } m_3 \geq 0 \\ L_{12} : 1 + m_{12} \to 1 \textit{ linear, deep and } 1\textit{-separated} \\ L_2 : m_2 \to 1 \quad \textit{linear and deep} \\ \hat{T} : m_{13} + m_{12} + m_3 + m_2 \to 1 \\ m_3 = 0 \implies L_2 \not\equiv \langle 0 \rangle_0 \end{array}$$

then for all $q : 0 \to 1$, $v_3 : 0 \to m_{13}$, $v_2 : 0 \to m_{12}$, *and* $e : 0 \to m_3$ *we have*

$$\begin{array}{l} \mathbf{par}_{2+m_3} \cdot (q + L_{12} \cdot (\mathbf{par}_{1+m_{13}} \cdot (\mathbf{id}_1 + v_3) + v_2) + e) \cdot s \\ \xrightarrow{\mathbf{par}_{2+m_3} \cdot (\mathbf{id}_1 + \mathbf{id}_{m_3} + L_2)} \mathbf{par}_2 \cdot (q + \hat{T} \cdot (v_3 + v_2 + \mathbf{ppar}_{m_3} \cdot (e + \mathbf{id}_{m_3}) + \mathbf{id}_{m_2})) \end{array}$$

Proof By the definitions of deep and shallow labelled transitions, using the fact that L_{12} is deep in argument 1 and is 1-separated to justify some cancellation steps. □

Lemma 34 *If* $s \xrightarrow{\mathbf{par}_{3+m_3} \cdot (\mathbf{id}_1 + \mathbf{id}_{m_3} + L_{12} + L_2)} \hat{T}$, *where*

$$\begin{array}{l} m_{12} \geq 0 \textit{ and } m_2 \geq 0 \textit{ and } m_3 \geq 0 \\ L_{12} : m_{12} \to 1 \textit{ linear and deep} \\ L_2 : m_2 \to 1 \quad \textit{linear and deep} \\ \hat{T} : m_3 + m_{12} + m_2 \to 1 \\ m_3 = 0 \implies L_2 \not\equiv \langle 0 \rangle_0 \end{array}$$

then for all $a' : 0 \to 1$, $v_2 : 0 \to m_{12}$, *and* $a''' : 0 \to m_3$ *we have*

$$\begin{array}{l} \mathbf{par}_{1+2+m_3} \cdot (s + a' + L_{12} \cdot v_2 + a''') \\ \xrightarrow{\mathbf{par}_{2+m_3} \cdot (\mathbf{id}_1 + \mathbf{id}_{m_3} + L_2)} \mathbf{par}_2 \cdot (a' + \hat{T} \cdot (\mathbf{ppar}_{m_3} \cdot (\mathbf{id}_{m_3} + a''') + v_2 + \mathbf{id}_{m_2})) \end{array}$$

Proof By the definition of shallow labelled transitions, using the fact that L_{12} and L_2 are deep to justify some cancellation steps. □

References

[1] Martín Abadi and Andrew D. Gordon. A calculus for cryptographic protocols: The spi calculus. In *Proceedings of the Fourth ACM Conference on Computer and Communications Security, Zürich*, pages 36–47. ACM Press, April 1997.

[2] S. Abramsky and L. Ong. Full abstraction in the lazy lambda calculus. *Information and Computation*, 105:159–267, 1993.

[3] Luca Aceto, Bard Bloom, and Frits Vaandrager. Turning SOS rules into equations. *Information and Computation*, 111(1):1–52, 15 May 1994.

[4] Franz Baader and Tobias Nipkow. *Term Rewriting and All That.* Cambridge University Press, New York, 1998.

[5] Jean-Pierre Banâtre and Daniel Le Métayer. A new computational model and its discipline of programming. Technical Report 566, INRIA, 1986.

[6] Karen L. Bernstein. A congruence theorem for structured operational semantics of higher-order languages. In *Proceedings of LICS 98*, 1998.

[7] Gérard Berry and Gérard Boudol. The chemical abstract machine. *Theoretical Computer Science*, 96:217–248, 1992.

[8] B. Bloom, S. Istrail, and A.R. Meyer. Bisimulation can't be traced. *Journal of the ACM*, 42(1):232–268, January 1995.

[9] Gérard Boudol. The π-calculus in direct style. In *Proceedings of the 24th POPL*, pages 228–241, 15–17 January 1997.

[10] Luca Cardelli and Andrew D. Gordon. Mobile ambients. In *Proc. of Foundations of Software Science and Computation Structures (FoSSaCS), ETAPS'98, LNCS 1378*, pages 140–155, March 1998.

[11] Gian Luca Cattani, A. John Power, and Glynn Winskel. A categorical axiomatics for bisimulation. In *Proceedings of CONCUR '98: Concurrency Theory (Nice). LNCS 1466*, September 1998.

[12] R. De Nicola and M. C. B. Hennessy. Testing equivalences for processes. *Theoretical Computer Science*, 34:83–133, 1984.

[13] R. de Simone. Higher-level synchronising devices in MEIJE–SCCS. *Theoretical Computer Science*, 37:245–267, 1985.

[14] U. Engberg and M. Nielsen. A calculus of communicating systems with label-passing. Technical Report DAIMI PB-208, Comp. Sc. Department, Univ. of Aarhus, Denmark, 1986.

[15] M. Felleisen and D. P. Friedman. Control operators, the SECD-machine and the λ-calculus. In *Formal Description of Programming Concepts III*, pages 193–217. North Holland, 1986.

[16] William Ferreira, Matthew Hennessy, and Alan Jeffrey. A theory of weak bisimulation for core CML. In *Proc. ACM SIGPLAN Int. Conf. Functional Programming.* ACM Press, 1996.

[17] Cédric Fournet and Georges Gonthier. The reflexive CHAM and the join-calculus. In *Proceedings of the 23rd POPL*, pages 372–385. ACM press, January 1996.

[18] Fabio Gadducci and Ugo Montanari. The tile model. In Gordon Plotkin, Colin Stirling, and Mads Tofte, editors, *Proof, Language and Interaction: Essays in Honour of Robin Milner.* MIT Press, 1999. To appear.

[19] R. J. van Glabbeek. The linear time – branching time spectrum. In *Proceedings of CONCUR '90, LNCS 458*, pages 278–297, 1990.

[20] R. J. van Glabbeek. The linear time – branching time spectrum II; the semantics of sequential systems with silent moves. In *Proceedings of CONCUR'93, LNCS 715*, pages 66–81, 1993.

[21] Andrew D. Gordon. Bisimilarity as a theory of functional programming. mini-course. Number NS-95-3 in the BRICS Notes Series, Computer Science Department, Aarhus, 1995.

[22] Andrew D. Gordon and Gareth D. Rees. Bisimilarity for a first-order calculus of objects with subtyping. In *Proceedings of the 23rd POPL*, pages 386–395, 1996.

[23] J.F. Groote and F.W. Vaandrager. Structured operational semantics and bisimulation as a congruence. *Information and Computation*, 100(2):202–260, 1992.

[24] Kohei Honda and Nobuko Yoshida. On reduction-based process semantics. *Theoretical Computer Science*, 152(2):437–486, 1995.

[25] Douglas J. Howe. Equality in lazy computation systems. In *Proceedings of LICS '89*, pages 193–203, 1989.

[26] Alex Mifsud. *Control Structures.* PhD thesis, University of Edinburgh, 1996.

[27] R. Milner, J. Parrow, and D. Walker. A calculus of mobile processes, Parts I + II. *Information and Computation*, 100(1):1–77, 1992.

[28] Robin Milner. Functions as processes. *Journal of Mathematical Structures in Computer Science*, 2(2):119–141, 1992.

[29] Robin Milner. Calculi for interaction. *Acta Informatica*, 33:707–737, 1996.

[30] Robin Milner and Davide Sangiorgi. Barbed bisimulation. In *Proceedings of 19th ICALP. LNCS 623*, pages 685–695, 1992.

[31] Ugo Montanari and Vladimiro Sassone. Dynamic congruence vs. progressing bisimulation for CCS. *Fundamenta Informaticae*, XVI:171–199, 1992.

[32] J. Niehren and M. Mueller. Constraints for free in concurrent computation. In *Proceedings of the Asian Computer Science Conference, LNCS 1023*, pages 171–186, 1995.

[33] Gordon D. Plotkin. A structural approach to operational semantics. Technical Report DAIMI FN-19, Computer Science Department, Aarhus University, Aarhus, Denmark, 1981.

[34] James Riely and Matthew Hennessy. A typed language for distributed mobile processes. In *Proceedings of the 25th POPL*, January 1998.

[35] Davide Sangiorgi. *Expressing Mobility in Process Algebras: First-Order and Higher-Order Paradigms.* PhD thesis, University of Edinburgh, 1993.

[36] Peter Sewell. On implementations and semantics of a concurrent programming language. In *Proceedings of CONCUR '97. LNCS 1243*, pages 391–405, 1997.

[37] Peter Sewell. From rewrite rules to bisimulation congruences. Technical Report 444, University of Cambridge, June 1998. Available from `http://www.cl.cam.ac.uk/users/pes20/`.

[38] Peter Sewell. From rewrite rules to bisimulation congruences. In *Proceedings of CONCUR '98: Concurrency Theory (Nice). LNCS 1466*, pages 269–284, September 1998.

[39] Peter Sewell. Global/local subtyping and capability inference for a distributed π-calculus. In *Proceedings of ICALP '98, LNCS 1443*, pages 695–706, 1998.

[40] A. Rensink. Bisimilarity of open terms. In *Expressiveness in Concurrency*, 1997. Full report version: Hildesheimer Informatik-Bericht 5/97, University of Hildesheim, May 1997.

[41] D. Turi and G.D. Plotkin. Towards a mathematical operational semantics. In *Proc. 12$^{\text{th}}$ LICS Conf.*, pages 280–291. IEEE, Computer Society Press, 1997.

[42] Femke van Raamsdonk. *Confluence and Normalisation for Higher-Order Rewriting.* PhD thesis, Vrije Universiteit, Amsterdam, 1996.