Weighted Relational Models for Mobility

James Laird*

Department of Computer Science, University of Bath, UK

Abstract

We investigate operational and denotational semantics for computational and concurrent systems with mobile names which capture their computational properties. For example, various properties of fixed networks, such as shortest or longest path, transition probabilities, and secure data flows, correspond to the "sum" in a semiring of the weights of paths through the network: we aim to model networks with a dynamic topology in a similar way. Alongside rich computational formalisms such as the λ-calculus, these can be represented as terms in a calculus of solos with weights from a complete semiring R, so that reduction associates a weight in R to each reduction path.

Taking inspiration from differential nets, we develop a denotational semantics for this calculus in the category of sets and R-weighted relations, based on its differential and compact-closed structure, but giving a simple, syntax-independent representation of terms as matrices over R. We show that this corresponds to the sum in R of the values associated to its independent reduction paths, and that our semantics is fully abstract with respect to the observational equivalence induced by sum-of-paths evaluation.

1998 ACM Subject Classification F.3.2 Semantics of Programming Languages, F.4.1 Mathematical Logic

Keywords and phrases Mobility, Concurrency, Solos

Digital Object Identifier 10.4230/LIPIcs.FSCD.2016.24

1 Introduction

Calculi based on name mobility [20, 23, 11] are well established as an elegant and expressive formalism for describing computation and communication in a broad range of concurrent systems. Semantics for these calculi, such as labelled transition systems, typically focus on local properties of processes – in particular, bisimulation equivalence. In this article we introduce resource-sensitive operational and denotational semantics for mobility which can capture quantitative properties of the whole system being modelled for a variety of potential resources (cost, security level, probability, . . .). Potentially, this will allow algorithmic reasoning principles developed for models such as weighted graphs to be extended to more dynamic systems.

1.1 Related Work

We will describe operational and denotational interpretations of the *solos calculus* [17] – that is, the fusion calculus [23] without any sequentialization in the form of input or output prefixing. The solos calculus presents name mobility in a particularly pure form, without any explicit notion of causal or temporal dependency, with an elegant graphical representation via *solo diagrams* [22]. However, Laneve and Victor [17] have shown that sequentialization

* Research supported by EPSRC grant EP/K037633/1.

1st International Conference on Formal Structures for Computation and Deduction (FSCD 2016).
Editors: Delia Kesner and Brigitte Pientka; Article No. 24; pp. 24:1–24:15
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

protocols may be written in the calculus using name-passing, recovering the expressive power of the π-calculus, for example, and establishing the solos calculus as an elegant and economical syntax for describing mobility in highly distributed systems.

We take inspiration from work by Ehrhard and Laurent [7], who have developed an interpretation of the solos calculus in the formal graphical language of *differential nets* [10], establishing a striking connections between name mobility and the differential structure [4] which underlies our model. There are some significant differences: our semantics includes replication (unlike the differential net semantics) but also the *acyclic* terms [7], which have some pathological behaviours.

We develop and extend work by Manzonetto, McCusker, Pagani and the author [16], which introduced operational and denotational semantics for nondeterministic functional programs with weights from a continuous semiring R. Each terminating reduction path in the operational semantics may be associated with a value in R by multiplying the weights ecountered, giving an interpretation of programs as a sum in R of the weights of their reduction paths. The corresponding denotational model in the category of free R-modules has differential structure, although this is not reflected in the syntax, leading to a failure of full abstraction. By moving to the solos calculus – with its close connection to differential structure – this paper develops an analogous, but fully abstract interpretation for a broader class of programs. (We show that there is a sound interpretation of R-weighted nondeterministic λ-terms in the solos calculus over R.)

Our semantics of a concurrent process calculus with mobility which represents terms as sums of their independent reduction paths is adumbrated by the work of Beffara [2], which captures directly this notion of independent path in the (finitary) πI-calculus, and uses it to give a trace semantics which is observed to possess many of the algebraic properties which we use to define our model (e.g. the processes over a given set of free names form a semiring). Our compositional construction of a semantics of this kind is therefore complementary, and opens up the question of defining a formal relationship with the trace semantics. Similarly, the representation of replication as a formal power series is foreshadowed by Boreale and Gadducci [5].

1.2 Contribution

In this paper we develop a new semantic account of the solos calculus, by weighting terms and reduction paths with values from a complete semiring R. Our main results are operational and denotational semantics for a "unidirectional" fragment of the calculus in which each closed term is interpreted as the sum in R of the weights of its reduction paths. We show that the unidirectional fragment is sufficiently expressive to capture reduction behaviour in the full calculus, and to evaluate sums-of-paths for an R-weighted non-deterministic λ-calculus.

Our denotational semantics interprets terms in the category of free R-modules and their homomorphisms, which correspond simply to matrices with entries in R. We formalize the differential structure required to interpret R-weighted unidirectional terms – a reflexive differential bialgebra – and use it to establish soundness of the model.

2 Preliminaries: Complete Semirings

Both operational and denotational semantics will use notions of complete monoid, semiring and semimodule, which we define here. A *complete monoid* [12] is a commutative monoid with infinite sums – a pair (S, Σ) of a set S with an operation Σ taking indexed[1] sets over S to elements of S, satisfying the following axioms:

- For any indexed family $\{a_i\}_{i \in I}$, and partitioning function $f : I \to J$, $\Sigma_{i \in I} a_i = \Sigma_{j \in J}(\Sigma_{i \in f^{-1}(j)} a_i)$.
- $\Sigma_{i \in \{j\}} a_i = a_j$.

A complete (commutative[2]) semiring R is a tuple $(|R|, \Sigma, \cdot, 1)$ such that $(|R|, \Sigma)$ is a complete monoid and $(|R|, \cdot, 1)$ is a commutative monoid which distributes over Σ – i.e. $a \cdot \Sigma_{i \in I} b_i = \Sigma_{i \in I} a \cdot b_i$.

If R is a complete semiring, then $(R, +, 0, \cdot, 1)$ is a commutative semiring in the usual sense (where 0 is the sum of the empty family, and $a_1 + a_2 = \Sigma_{i \in \{1,2\}} a_i$). R is *idempotent* if $a_i = b$ for all $i \in I$ implies $\Sigma_{i \in I} a_i = b$.

If the sub-semiring of R, of elements generated from the unit 1 is a semifield, then we may define an *exponential* function on R (a homomorphism from its additive to its multiplicative structure) as follows:

▶ **Definition 1.** Let R be a complete semiring. For each natural number n, let n_R denote the sum $\Sigma_{1 \leq i \leq n} 1$. If n_R has a multiplicative inverse $\frac{1}{n_R}$ for each $n > 0$, we may define the *Taylor exponential* $! : (R, +, 0) \to (R, \cdot, 1)$ as the sum of the formal power series $!a = \Sigma_{n \geq 0} \frac{1}{!n}.a^n$.

Note that we may define the Taylor exponential on any idempotent complete semiring (as $n_R = \frac{1}{n_R} = 1$ for all n).

2.1 Semiring-Weighted Networks

We shall represent concurrent systems as (possibly infinite) *matrices* over a complete semiring R (an $A \times B$ matrix over R is a function from $A \times B$ to R). To motivate the rest of the paper, we note that such matrices provide a general setting for defining and studying shortest-path and related problems [21], which are a classical application of semirings in quantitative analysis of static systems. An $A \times A$ matrix $G \in R^{A \times A}$ corresponds to a network, or weighted digraph on the set of nodes A, with $G(a, a')$ being the weight of the edge from a to a'. For any *path* (sequence of length at least 2) in A^* we may compute a weight by multiplication in R – i.e. $w(a_0, \ldots, a_{n+1}) = G(a_0, a_1) \cdot \ldots \cdot G(a_n, a_{n+1})$ – and so define the sum of weights of all paths between a and a': $\Sigma_G(a, a') = \Sigma_{s \in A^*} w(asa')$. The significance of this value depends on the choice of R. For example:

- If R is the *Boolean semiring* $\mathbb{B} = (\{\top, \bot\}, \bigvee, \wedge, \top)$ (i.e. G represents an unlabelled digraph) then $\Sigma_G(a, a') = \top$ iff there is a path from a to a'.
- In general, if R is a *lattice*, (e.g. $G(a, a')$ is the security level of information that can pass from a to a') then $\Sigma_G(a', a)$ is the least upper bound of all information that may flow from a to a'
- If R is the *tropical semiring* $\mathbb{T}^\infty = (\mathbb{R}_+ \cup \{\infty\}, \bigwedge, +, 0)$ (i.e. $G(a, a')$ is the length or cost of travelling from a to a') then $w(s)$ represents the length of the path s and $\Sigma_G(a, a')$ is the length of the shortest path from a to a'.
- If R is the *probability semiring* $(\mathbb{R}_+ \cup \{\infty\}, \Sigma, \times, 1)$, and the sum of weights entering (or leaving) each node is less than 1 (i.e G is a *stochastic matrix*) then $\Sigma_G(a, a')$ is the probability of reaching a' from a.

[1] Our semantics restrict straightforwardly to countably complete monoids/semirings.
[2] Only commutative monoids and semirings will be considered throughout.

3 A Calculus of Solos With Resources

In this section we describe a "resource sensitive" version of the *solos calculus* [17]. This is the fragment of the fusion calculus [23] without prefixing – that is, we have primitives (solos) which can emit or receive channel names, but no primitives for expressing sequentialization (although these may be expressed). We include *weights* from a commutative monoid, which can quantify the resources used (the monoid operation shows how to combine weights across parallel composition).

We work in the *dyadic*[3] solos calculus, omitting matching of channel names, but including *explicit fusions* of names, which simplify presentation of the semantics (these are studied in detail by Wischik and Gardner [25]). Let $M = (|M|, \cdot, 1)$ be a commmutative monoid. Terms of the solos calculus over M are formed according to the grammar:

$$p, q ::= \underline{a} \mid x(y,z) \mid \overline{x}(y,z) \mid x = y \mid p|q \mid p + q \mid\, !p \mid \nu x.p$$

where variables x, y, z represent communication channel names, and:

- Each constant $\underline{a}$ is a *weight* representing the value a in $|M|$.
- $x(y,z)$ and $\overline{x}(y,z)$ are input and output *solos* – representing the receiving and sending of the pair of names y and z on the channel x, respectively.
- $x = y$ is an *explicit fusion* asserting the identity of the names x and y.
- $p|q$ is *parallel composition*, with unit $\underline{1}$.
- $\nu x.p$ is *hiding*, binding the name x in p.
- $!p$ is the *exponential* of p, offering arbitrarily many copies of p in parallel.
- $p + q$ is an (external) *choice* of the processes p and q.

3.1 Reduction Semantics

Our operational semantics for the solos calculus is non-standard – the primary justification for this is that it reflects an elegant denotational, *algebraic* model. The close correspondence between the calculus and *differential nets* [10, 8] suggests that a term of the solos calculus can represent a collection of resources, so that reduction determines whether these resources are successfully consumed or not (as in the differential λ-calculus [9]). In practical terms, this means that our reduction rules for the solos calculus are linear, rather than affine – a resource which cannot be consumed (e.g. $\nu x.x(y,z)$) is not equivalent to the unit for parallel composition – and the sum is an external choice corresponding to the sum in a semiring. Note that the latter may be macro-expressed (e.g. as $p + q = \nu x.\overline{x}(-,-)|!(x(-,-)|p)|!(x(-,-)|q)$ where x is not free in p or q). Linearity allows us to be more precise about how resources are used, but we can express the affine behaviour of the original solos calculus (e.g. by representing an affine solo as a choice $x(y,z) + 1$), as for the π-calculus [2].

We work up to *structural congruence*, which is the smallest congruence on terms containing α-equivalence with respect to bound variables and the following axioms:

$$\begin{array}{llll} p|(q|r) \equiv (p|q)|r & p|q \equiv q|p & p|\underline{1} \equiv p & \underline{a}|\underline{b} \equiv \underline{a \cdot b} \\ \nu x.\nu y.p \equiv \nu y.\nu x.p & \nu x.\underline{1} \equiv \underline{1} & (\nu x.p)|q \equiv \nu x.(p|q)\ (x \notin FV(p)) & \end{array}$$

In other words, terms are identified up to associativity and commutativity of parallel composition (which acts as multiplication in M on weights) and scope extrusion of variables. The basic reduction rules are as follows:

[3] This is a minimal, expressive version of the calculus – Laneve and Victor [17] show that monadic solos cannot express polyadic solos.

$$\overline{x}(u,v)|x(y,z) \to u = y|z = v$$
$$!p \to \underline{1} \qquad \nu x.x = y|p \to p[y/x] \qquad p + q \to p$$
$$!p \to p|!p \qquad \nu y.x = y|p \to p[x/y] \qquad p + q \to q$$

In other words, communicating solos reduce by fusing their arguments, $!p$ may replicate or discard p,[4] explicit fusion of a bound variable reduces by substitution with the variable to which it is fused and non-deterministic choice reduces to one of its branches.

These reductions may be applied inside hiding and parallel composition, to terms identified up to structural congruence. We define the compatible reduction $\longrightarrow$ to be the least relation on terms such that:

$$\frac{p \to q}{p \longrightarrow q} \qquad \frac{p \equiv p' \quad p \longrightarrow q \quad q \equiv q'}{p' \longrightarrow q'} \qquad \frac{p \longrightarrow q}{\nu x.p \longrightarrow \nu x.q} \qquad \frac{p \longrightarrow q}{p|r \longrightarrow q|r}$$

Every terminating reduction path ends either in a weight $\underline{a}$ or an irreducible term p which contains solos which cannot communicate – i.e. resources which cannot be consumed or demands for resources which cannot be satisfied (cf. the differential λ-calculus [9]). In the former case, we say that a is a weight for the path, in the latter, that p is a *failure* (written $p \not\downarrow$).

For instance, we might represent a finite directed graph with weights from M as a term of the solos calculus, such that reduction paths correspond to paths through G. Assuming for the sake of simplicity that G is acyclic, let $\widetilde{G} = |_{i,j \in N}!([x_i \mapsto x_j]|a_{ij})$,

▶ **Proposition 2.** *$\nu x_1 \ldots x_n.\overline{x_1}(-,-)|\widetilde{G}|x_k(-,-) \downarrow a$ if and only if there is a path from node 1 to node k of weight a.*

More importantly, using the solos calculus allows us to describe networks which do not have a fixed topology – for example by passing names *through* the network to create new (weighted) connections.

3.2 The Unidirectional Solos Calculus

Our aim is to give a semantics of the solos calculus which accounts for all reduction paths, by summing their weights in a complete semiring. In general, to compute a sum of path weights for a term it is necessary to take account of the *multiplicity* of distinct paths to the same value, where paths are distinguished according to the different choices made during reduction, but not the order in which they are made. To make this notion of "sum of independent paths" precise, we restrict attention to an expressive fragment of the solos calculus, closer to differential nets, for which we are able to give operational and denotational semantics which give a consistent interpretation of path sum. This "unidirectional" fragment is defined by a derivation system which separates input and output capabilities and enforces constraints on mobility of names related to those in the private π-calculus [24].

In a unidirectional term, the solo $\overline{x}(y,z)$ is assumed to send (on x) the capability to receive on y and send on z. Accordingly, we say that x and z occur as output names, and y as an input name in $\overline{x}(y,z)$. Dually $x(y,z)$ receives on x the capability to send on y, and receive on z – i.e. x and z occur as input names and y as an output name. The fusion $x = y$ joins an input name (x) to an output name (y).

We shall say that an occurrence of a variable is *mobile* if it is the argument to an input or output solo, or in an explicit fusion – i.e. y, z occur as mobile names in both $x(y,z)$,

[4] Note that $!p$ is *not* structurally congruent to $p|!p$, reflecting the linear nature of our rules.

$$\frac{}{x,\underline{z}\vdash x(y,z);\underline{y}} \qquad \frac{}{\underline{y}\vdash \overline{x}(y,z);x,\underline{z}} \qquad \frac{}{\underline{x}\vdash x{=}y;\underline{y}}$$

$$\frac{\Gamma\vdash p;\Delta}{\Gamma-\{x\}\vdash \nu x.p;\Delta-\{x\}} \qquad \frac{\Gamma\vdash p;\Delta \quad \Gamma\vdash q;\Delta}{\Gamma\vdash p+q;\Delta} \qquad \frac{}{\_\vdash a;\_}\, a\in|M|$$

$$\frac{\Gamma\vdash p;\Delta \quad \Gamma'\vdash q;\Delta'}{\Gamma\cup\Gamma'\vdash p|q;\Delta\cup\Delta'}\,\Gamma\between\Gamma',\Delta\between\Delta' \qquad \frac{\Gamma\vdash p;\Delta}{\Gamma\vdash !p;\Delta}\,\underline{\Gamma}=\underline{\Delta}=\varnothing$$

Figure 1 Derivation Rules for Unidirectional Solos.

$\overline{x}(y, z)$ (and $y = z$), whereas x does not. A unidirectional context Γ is a set of names with a specified subset $\underline{\Gamma} \subseteq \Gamma$ of mobile names. Figure 1 gives derivation rules for unidirectional terms-in-context of the form $\Gamma \vdash p; \Delta$, where Γ and Δ are unidirectional contexts of input and output names occurring in p. These rules may be seen as enforcing a simple *linear* typing discipline on terms of the solos calculus: mobile names must be used linearly, whereas static names may be used freely, with respect to the input and output modalities separately.

We write $\Gamma \between \Gamma'$ if $\underline{\Gamma} \cap \Gamma' = \varnothing$ and $\underline{\Gamma'} \cap \Gamma = \varnothing$. Sharing of mobile names is constrained by requiring that in the parallel composition $p|q$ the input and output contexts of p and q must be non-interfering in this sense. Similarly, the exponential $!p$ may contain no (free) mobile names. A name is static in $\Gamma \vdash p; \Delta$ if it does not occur in $\underline{\Gamma} \cup \underline{\Delta}$.

▶ **Proposition 3.** *If $\Gamma \vdash p; \Delta$ and $p \longrightarrow q$ then there exist Γ', Δ' such that $\Gamma' \vdash p; \Delta'$.*

Proof. This is evident for the basic reductions of communicating solos, choice and replication. The key case is reduction of explicit fusion by substitution. We show that if $\Gamma, y \vdash p; \Delta, x$, where $x \notin \Gamma$ and $y \notin \Delta$, then $\Gamma, y \vdash p[y/x]; \Delta, y$ by induction on p. Hence if $\Gamma, y \vdash \nu x.x = y|p; \Delta, \underline{y}$, so that $\Gamma, y \vdash p; \Delta, x$ then $\Gamma, y \vdash p[y/x]; \Delta, y$ as required. (Note, however, that in this case, y is now output-static.)

It is straightforward to check that unidirectionality is preserved under structural congruence – i.e. if $p \equiv p'$ and $\Gamma \vdash p; \Delta$ then $\Gamma \vdash p'; \Delta$. So subject reduction extends to the compatible reduction relation. ◀

We now assume that our monoid of resources is the multiplication in a complete semiring R with a Taylor exponential.

3.3 Expressiveness of Unidirectional Terms

Passing of bound names, as in the private π-calculus [24], is naturally expressed in the unidirectional fragment: we write $x(\underline{y}, \underline{z})p$ and $\overline{x}(\underline{y}, \underline{z})p$ for $\nu y.\nu z.x(y, z)|p$ and $\nu y.\nu z.\overline{x}(y, z)|p$ respectively. These are essentially bound input and output operations for the "synchronous π-calculus" [3].

To show the expressiveness of the unidirectional solos calculus , we may define unidirectional terms which correspond to bidirectional solos – i.e. they can pass the capability to send and receive on static names. Hence we may give a translation of the full solo calculus into the unidirectional fragment which is sound with respect to reduction.

Using the *forwarder* $[x \mapsto y] =_{df} \nu u.\nu v.x(u, v)|\overline{y}(u, v)$, we may define macros for explicit fusions of static variables (the *equators* of [14]) – let $\widehat{x = y} =_{df} ![x \mapsto y]|![y \mapsto x]$ – and for monadic bidirectional solos $\widehat{x(u)}$ (input) and $\widehat{\overline{x}(u)}$ (output) which pass both input and output capabilities on the static name u:

$\widehat{x(u)} =_{df} x(\underline{v}, \underline{w})![v \mapsto u]|![u \mapsto w]$ $\qquad$ $\widehat{\overline{x}(u)} =_{df} \overline{x}(\underline{v}, \underline{w})![u \mapsto v]|![w \mapsto u]$ We define a unidirectional term representing the dyadic bidirectional solo $x(y, z)$ by passing private names v, w on x, and communicating send and receive capacity for y on v, and for z on w (as in the encoding of polyadic communication in the monadic π-calculus [24]) – i.e.

- $\widehat{x(y, z)} = x(\underline{v}, \underline{w})\widehat{v(y)}|\widehat{\overline{w}(z)}$.
- $\widehat{\overline{x}(y, z)} = \overline{x}(\underline{v}, \underline{w})\widehat{\overline{v}(y)}|\widehat{w(z)}$.

This yields a compositional translation $\widehat{\_}$ of the (dyadic) solos calculus into its unidirectional fragment by replacing each solo and explicit fusion with the corresponding macro.

▶ **Proposition 4.** *For every term p, $p \longrightarrow^* \underline{a}$ if and only if $\widehat{p} \longrightarrow^* \underline{a}$.*

Proof Outline. We show the following by induction on reduction:

- for any unidirectional term p, $\nu x.\widehat{x = y}|p \longrightarrow^* \underline{a}$ if and only if $\nu x.p[x/y] \longrightarrow^* \underline{a}$. (We prove from left to right by showing that if $\nu x.([x \mapsto y]|[y \mapsto x])^n|\widehat{x = y}|p \longrightarrow^* \underline{a}$ for some n then $\nu x.p[x/y] \longrightarrow^* \underline{a}$.)
- $\nu x.\widehat{v(y)}|\widehat{\overline{v}(y')}|\widehat{p} \longrightarrow^* \underline{a}$ if and only if $\widehat{y = y'}|\widehat{p} \longrightarrow^* \underline{a}$.
- $\widehat{x(y, z)}|\widehat{\overline{x}(y', z')}|\widehat{p} \longrightarrow^* \underline{a}$ if and only if $\widehat{y = y'}|\widehat{z' = z}|\widehat{p} \longrightarrow^* \underline{a}$.

In other words, reduction of $\widehat{p}$ precisely tracks reduction of p, and hence $p \longrightarrow^* \underline{a}$ if and only if $\widehat{p} \longrightarrow^* \underline{a}$. ◀

3.4 The Quantitative λ-Calculus

As a demonstration of the expressiveness of quantitative unidirectional solos, we adapt Milner's translation of the λ-calculus into the π-calculus [19]. [16] introduced an applied λ-calculus (PCF) with non-deterministic choice and scalar multiplication by weights in a continuous semiring R, describing an operational semantics evaluating programs to elements of R and a corresponding denotational semantics in the category of weighted relations (i.e. matrices) over R (which will also furnish models of the solos calculus over R). We show that these results may be recast as an interpretation of the untyped λ-calculus with choice in the unidirectional solo calculus (where they may be extended to any *complete* semiring with a Taylor exponential).

For any complete semiring R, let Λ^+_{R} be the (lazy) λ-calculus extended with a binary choice operator $+$, and weighting with values from R – i.e. terms are given by the grammar:

$$M, N ::= x \mid \lambda x.M \mid M\, N \mid M + N \mid \underline{a}(M)$$

where a ranges over elements of R.

We may interpret Λ^+_{R} by translation into the unidirectional solos calculus over R . A term M of Λ^+_{R} over the free variables $x_1, \ldots, x_n$ is interpreted as a R-term $x_1, \ldots, x_n \vdash (\!|M|\!)(u); u$ with free static input names $x_1, \ldots, x_n$ and output name u.

- $(\!|x|\!)(u) = x(u, -)$
- $(\!|\lambda x.M|\!)(u) = !\overline{u}(\underline{v}, \underline{x})(\!|M|\!)(v)$
- $(\!|M\, N|\!)(u) = \nu v.v(u, \underline{w})|(\!|M|\!)(v)|!\overline{w}(\underline{y}, -)(\!|N|\!)(y)$.
- $(\!|M + N|\!)(u) = (\!|M|\!)(u) + (\!|N|\!)(u)$.
- $(\!|\underline{a}(M)|\!)(u) = \underline{a}|(\!|M|\!)(u)$.

We show that this translation is sound with respect to an operational semantics of Λ^+_{R} which evaluates each term to the sum of its reduction-path weights (based on [16]).

4 Denotational Semantics

We now describe, for each complete semiring R, a fully abstract interpretation of the unidirectional solos calculus in the symmetric monoidal category Mat_R of sets and matrices over R. The objects of Mat_R are sets, and morphisms from X to Y are $X \times Y$ matrices (a.k.a. "R-weighted relations") over R, composed by matrix multiplication – given $f : X \to Y$ and $g : Y \to Z$, $(f; g)(x, z) = \Sigma_{y \in Y} f(x, y) \cdot g(y, z)$.

The tensor product $X \otimes Y$ is the cartesian product of X and Y as sets (with unit I being the singleton set), sending $f : X \to X'$ and $g : Y \to Y'$ to the matrix $f \otimes g$ with $(f \otimes g)(x, y, x', y') = f(x, x') \cdot g(y, y')$. Mat_R is *compact closed*: every object Y is dual to itself – i.e. there are evident natural isomorphisms $\mathsf{Mat}_\mathrm{R}(X \otimes Y, Z) \cong \mathsf{Mat}_\mathrm{R}(X, Y \otimes Z)$.

For each X, Y, the $X \times Y$ matrices over R form a *R-module* – that is, a complete monoid with an operation of scalr multiplication by elements of R, which satisfies:

$$(\Sigma_{i \in I} a_i).u = \Sigma_{i \in I}(a_i.u) \qquad a.\Sigma_{i \in I} u_i = \Sigma_{i \in I} a.u_i \qquad (a \cdot b).u = a.(b.u) \qquad (1.u) = u$$

▶ **Proposition 5.** Mat_R *is enriched over the category of R-modules and their homomorphisms.*[5]

Proof. Concretely, this means that there are indexed sum and scalar multiplication operations on each hom-set (i.e. pointwise addition and multiplication of matrix entries) which satisfy the axioms for a R-module and distribute over composition and the tensor product – i.e.

- $(\Sigma_{i \in I} f_i); g = \Sigma_{i \in I} f_i; g$, $f; \Sigma_{j \in J} g_j = \Sigma_{j \in J}(f; g_j)$ and $(a.f); g = a.(f; g) = f; (a.g)$.
- $(\Sigma_{i \in I} f_i) \otimes g = \Sigma_{i \in I}(f_i \otimes g)$ and $(a.f \otimes g) = a.(f \otimes g)$.

By elementary linear algebra, the embedding of Mat_R into the category of R-modules which sends each set X to the free R-module R^X, and each $X \times Y$ matrix to the corresponding linear function from R^X to R^Y is fully faithful. ◀

4.1 Differential Structure

We interpret sharing of channels (contraction and weakening) using simple *differential structure* in our category of matrices. The properties we require may be presented as follows:

▶ **Definition 6.** A *differential bialgebra* on a pair of objects (A, B) in a commutative-monoid-enriched symmetric monoidal category is given by morphisms $(\mu : B \otimes B \to B, \eta : I \to B, \delta : B \to B \otimes B, \epsilon : B \to I, \zeta : A \to B, \xi : B \to A)$ such that $(B, \mu, \eta, \delta, \eta)$ is a *commutative bialgebra*, and the following equations hold:

(i) $\zeta; \xi : A \to A = \mathsf{id}_A$
(ii) $\eta; \xi : I \to A = 0$ and $\zeta; \epsilon : A \to I = 0$
(iii) $\mu; \xi : B \otimes B \to A = (\epsilon \otimes \xi) + (\xi \otimes \epsilon)$ and $\zeta; \delta : A \to B \otimes B = (\eta \otimes \zeta) + (\zeta \otimes \eta)$

These equations are implicit in the definition of differential nets [10], and included explicitly (alongside further structure) in the notion of a *model of the differential calculus* [4], which is proven equivalent to a *differential category with a storage modality* – in any such category there is a comonad $! : A \to A$ with a differential bialgebra on $(A, !A)$ for each A. In Mat_R we may define a differential bialgebra on $(A, \mathcal{M}_*(A))$ for any set A, where $\mathcal{M}_*(A)$ is the set of *finite multisets* over A, by following the construction of the *cofree commutative comonoid* on [18, 16] (essentially, a generalization of the finite multiset exponential on the relational model of linear logic). Specifically, we may define the matrices:

[5] The category of R-modules and their homomorphisms is symmetric monoidal closed, with construction of the tensor product of R-modules following [13] – see e.g. [1] for extension with infinite sums).

- $\eta(*, X) = \epsilon(X, *) = 1$ if $X = \{\}$, 0 otherwise.
- $\mu((X, Y), Z) = \delta(X, (Y, Z)) = 1$ if $X = Y \uplus Z$, 0 otherwise.
- $\xi(X, x) = \zeta(x, X) = 1$ if $X = \{x\}$, 0 otherwise.

We interpret (the "type" of) channels as a differential bialgebra which satisfies a basic recursive equation: on a channel we may send (finitely but unboundedly many) pairs of an output and input name.

▶ **Definition 7.** A *reflexive* differential bialgebra is an object B (in a commutative monoid-enriched SMC) with a *dual* B^* and a differential bialgebra on $(B \otimes B^*, B)$.

To define a reflexive differential bialgebra in $\mathsf{Mat}_{\mathrm{R}}$, we take the least fixed point of the $\subseteq$-continuous operation sending the set X to the set $\mathcal{M}_*(X \times X)$ of finite multisets of pairs of elements of X. Let B be the (countable) set $\bigcup_{i \in \omega} B_i$, where $B_0 = \varnothing$, and $B_{i+1} = \mathcal{M}_*(B_i \times B_i)$, so that $B = \mathcal{M}_*(B \times B)$. Since B is self-dual, and the tensor product in $\mathsf{Mat}_{\mathrm{R}}$ is cartesian product of sets, $B = \mathcal{M}_*(B \otimes B^*)$.

4.2 Denotational Interpretation

Let R be a complete semiring with a Taylor exponential, and let B be a reflexive differential bialgebra in a R-module-enriched symmetric monoidal category $\mathcal{C}$, yielding a commutative bialgebra $(B^{\otimes n}, \mu_n, \eta_n, \delta_n, \epsilon_n)$ for each n.

For each m, n, $\mathcal{C}(B^{\otimes m}, B^{\otimes n})$ is a complete semiring – we may define a product operation on $\mathcal{C}(B^{\otimes m}, B^{\otimes n})$: $f \cdot g = \delta_m; (f \otimes g); \mu_n$, with neutral element $1 = \epsilon_m; \eta_n : B^{\otimes m} \to B^{\otimes n}$. This is associative and commutative, and distributes over the indexed sum on $\mathcal{C}(B^{\otimes m}, B^{\otimes n})$, yielding a complete semiring $\mathcal{C}_{\mathrm{R}}(B^{\otimes m}, B^{\otimes n})$, with a homomorphism of semirings from R into $\mathcal{C}_{\mathrm{R}}(B^{\otimes m}, B^{\otimes n})$ sending $a \in R$ to $a.1$. Hence, in particular, $\mathcal{C}_{\mathrm{R}}(B^{\otimes m}, B^{\otimes n})$ has a Taylor exponential. The full subcategory of $\mathcal{C}$ generated from I, B, B^* is compact closed, and therefore has a canonical *trace operator* [15], with which we interpret hiding.

Ordering input and output contexts, we interpret terms-in-context $x_1, \ldots, x_m \vdash p; x_1, \ldots, x_n$ in $\mathcal{C}_{\mathrm{R}}(B^{\otimes m}, B^{\otimes n})$, as follows:

- *Constants* denote scalar multiples of the unit: $[\![\_ \vdash \underline{a}; \_]\!] = k.\mathsf{id}_I$.
- *Solos* denote ξ and ζ: $[\![x, z \vdash x(y, z); y]\!] = \Lambda^{-1}(\xi)$, $[\![y \vdash \overline{x}(y, z); x, z]\!] = \Lambda(\zeta)$.
- *Explicit Fusions* denote the identity: $[\![x \vdash x = y; y]\!] = \mathsf{id}_B$.
- *Hiding* denotes the trace operation: $[\![\Gamma \vdash \nu x.p; \Delta]\!] = \mathrm{tr}([\![\Gamma, x \vdash p; \Delta, x]\!])$.
- *Composition* denotes the product: $[\![\Gamma \vdash p|q; \Delta]\!] = [\![\Gamma \vdash p; \Delta]\!] \cdot [\![\Gamma \vdash q; \Delta]\!]$.
- *Choice* denotes the sum: $[\![\Gamma \vdash p + q; \Delta]\!] = [\![\Gamma \vdash p; \Delta]\!] + [\![\Gamma \vdash q; \Delta]\!]$.
- *Replication* denotes the Taylor exponential: $[\![\Gamma \vdash !p; \Delta]\!] = ![\![\Gamma \vdash p; \Delta]\!]$.

Permutation of contexts corresponds to composition with the corresponding isomorphisms on $B^{\otimes m}$ and $B^{\otimes n}$, and weakening of contexts to composition with $B^{\otimes m} \otimes \epsilon : B^{\otimes m+1} \to B^{\otimes m}$ and $B^{\otimes n} \otimes \eta : B^{\otimes n} \to B^{\otimes n+1}$

It may be noted that this interpretation does not mention unidirectionality. However, it plays a critical role in the proof of its *soundness* in the following section.

5 Sum-of-Paths Evaluation

We now aim to show that our denotational semantics for a (closed) unidirectional term p over the semiring R corresponds to an operational semantics which computes a sum in R of the residues of the reduction paths of p.

$$\frac{}{\underline{a} \Downarrow_{\mathrm{R}} a} \qquad \frac{p \Downarrow_{\mathrm{R}} a \quad p \equiv q}{q \Downarrow_{\mathrm{R}} a} \qquad \frac{p \not\downarrow}{p \Downarrow_{\mathrm{R}} 0}$$

$$\frac{p \Downarrow_{\mathrm{R}} a}{\nu x.p \Downarrow_{\mathrm{R}} a} \qquad \frac{p|r \Downarrow_{\mathrm{R}} a \qquad q|r \Downarrow_{\mathrm{R}} b}{(p+q)|r \Downarrow_{\mathrm{R}} a+b} \qquad \frac{p^n|q \Downarrow_{\mathrm{R}} a_n}{!p|q \Downarrow_{\mathrm{R}} \Sigma_{n \geq 0} \frac{a_n}{n!}}$$

$$\frac{p \Downarrow_{\mathrm{R}} a}{x{=}x|p \Downarrow_{\mathrm{R}} \infty.a} \qquad \frac{x(y_1,z_1)|\ldots|u{=}y_i|z_i{=}v|\ldots|x(y_n,z_n)|p \Downarrow_{\mathrm{R}} a_i}{\overline{x}(u,v)|x(y_1,z_1)|\ldots|x(y_n,z_n)|p \Downarrow_{\mathrm{R}} \Sigma_{i \leq n} a_i}\; x \notin FV^-(p) \qquad \frac{p[y/x] \Downarrow_{\mathrm{R}} a}{x{=}y|p \Downarrow_{\mathrm{R}} a} x \not\equiv y$$

Figure 2 Evaluation Rules for Unidirectional Terms.

If R is idempotent, then we may define this to be $\bigvee\{a \mid p \downarrow a\}$, but in the general case, we require a notion of (syntax) *independent reduction path*. On the one hand, it is necessary to take account of the *multiplicity* of distinct paths to the same value. For example, there should be two reduction paths from $\underline{a} + \underline{a}$ to $\underline{a}$. On the other hand some distinct reduction paths in the rewriting system are different syntactic representations of the same events and so do not represent independent paths in the required sense. For example, there is a single path from $\underline{a} + \underline{b}|\underline{c} + \underline{d}$ to $\underline{a}|\underline{c}$. Moreover, in calculi with mobility such as the solos calculus the order in which reduction choices are made changes the communications available – as in the term $\nu x \nu y.\nu z.x(y, z)|\overline{x}(z, y)|y(x, z)|\overline{y}(z, x)|z(x, y)|\overline{z}(y, x)$, for example.

Beffara makes this notion of independent reduction path *explicit* in giving a trace semantics of the πI-calculus [2], which is quotiented by an equivalence relation between reduction paths. However, if p is a term in our unidirectional solos calculus we can always find a channel on which *all possible interactions are simultaneously available*, and so it remains implicit in the operational semantics given here.

▶ Remark. Unidirectionality, and our denotational semantics, provide a perspective on the notion of *acyclicity* introduced by Ehrhard and Laurent [7]. Cycles arise when a channel name becomes fused to itself – a term is acyclic if it never attempts to fuse a channel to itself in this way.

In our semantics, cyclic terms denote infinite sums of paths. For example, consider the solo term $\nu x.x = x$, which denotes the composition of the unit and counit $\nu_B; \epsilon_B : I \Rightarrow I$. Letting $\infty = \Sigma_{i \in \mathbb{N}} 1$ (note that if R is idempotent, then $\infty = 1$) then $\Sigma_{b \in B} \mathsf{id}_I = \infty.\mathsf{id}_I$, whereas (e.g.) $\nu x.\nu y.x = y$ denotes id_I. Semantically, this corresponds to identifying an explicit fusion such as $x = x$ with the forwarder $![x \mapsto x]$, which reduces to $\nu yz.x(y, z)|\overline{x}(y, z)|![x \mapsto x] \longrightarrow \nu yz.y = y|z = z|![x \mapsto x]$, generating infinitely many reduction paths. Note that this does not arise for forwarders and equators in the π-calculus, which must receive an input before they can send an output – more generally (as noted by Ehrhard and Laurent), terms of the π-calculus and λ-calculus can be represented as acyclic solos.

5.1 Evaluation Semantics

The rules in Figure 2 define a relation $\Downarrow_{\mathrm{R}}$ between unidirectional R-terms and values in R, such that if $p \Downarrow_{\mathrm{R}} a$ then a is the sum in R of the weights of the reduction paths of p. We write p^n for the composition of n copies of p – i.e. $p^0 = 1$, $p^{n+1} = p|p^n$, and $FV^-(p)$ for the set of input names of p.

▶ **Proposition 8.** *For any term p, there exists a such that $p \Downarrow_R a$.*

Proof. By induction on the (well-founded [6]) multiset ordering on the measure $\ell(p)$, defined as follows:

$$\ell(\underline{a}) = \ell(x = y) = \varnothing \qquad \ell(x(y,z)) = \ell(\overline{x}(y,z)) = \{\{\}\}$$
$$\ell(\nu x.p) = \ell(p) \qquad \ell(p|q) = \ell(p) \cup \ell(q)$$
$$\ell(p+q) = \ell(p) \cup \ell(q) \cup \{\{\}\} \qquad \ell(!p) = \{\ell(p)\}$$

Note that ℓ is invariant with respect to structural congruence, and if $q \Downarrow_{\mathrm{R}} b$ is a premise for a rule (other than structural congruence) with conclusion $p \Downarrow_{\mathrm{R}} a$, then $\ell(q) \ll \ell(p)$. If p contains occurrences of $!$, $=$ or $+$, then one of the corresponding rules is applicable. Otherwise p is equivalent to $\nu x_1 \ldots \nu x_m.p'$, where p' is a parallel composition of solos and constants. If p' consists only of constants, then $p \equiv \underline{a}$ for some a. If p' contains a pair of complementary solos $x_i(x_j, x_k)$ and $\overline{x_i}(x_{j'}, x_{k'})$ then by unidirectionality x_i cannot occur as a mobile name in p', and so the communication rule applies. Otherwise p is a failure. ◀

Moreover, it is a consequence of the soundness of the denotational model (Proposition 17) that the result of evaluation is unique and therefore $\Downarrow_{\mathrm{R}}$ defines a function from closed R-terms to elements of R. For idempotent complete semirings, this agrees with small-step reduction in the following sense.

▶ **Proposition 9.** *If R is idempotent, $p \Downarrow_R \bigvee\{k \mid p \longrightarrow^* \underline{a}\}$*

Proof. By induction over the nested multiset ordering on $\ell(p)$. ◀

Each complete semiring R induces a notion of contextual equivalence (R-equivalence) on unidirectional solo terms, by testing closed terms with $\Downarrow_{\mathrm{R}}$. Say that a context $C[\_]$ is a closing context for Γ, Δ if for any unidirectional term $\Gamma \vdash p; \Delta$, $C[p]$ is a closed unidirectional term.

▶ **Definition 10.** Given terms $\Gamma \vdash p, q; \Delta$, $p \sim_{\mathrm{R}}^{\Gamma,\Delta} q$ if for all closing contexts $C[\_]$ for Γ, Δ, $C[p] \Downarrow_{\mathrm{R}} a$ if and only if $C[q] \Downarrow_{\mathrm{R}} a$.[6]

The properties of $\sim_{\mathrm{R}}$ depend on R, but in general it is neither coarser nor finer than the bisimulation equivalence for the solos calculus [17]. We give some illustrative examples of equivalences and inequivalences (for non-trivial R), which follow from full abstraction of the denotational semantics. We leave the input and output contexts implicit.

- *Units* $\underline{1} \not\sim_{\mathrm{R}} \underline{0}$ – as noted, our interpretation of solo terms is not *affine*.
  $p|\underline{0} \sim_{\mathrm{R}} \underline{0}$ – $\underline{0}$ is an absorbing element for parallel composition.
- *Choice* $p|(q+r) \sim_{\mathrm{R}} p|q + p|r$ (distributivity).
  $p + p \sim_{\mathrm{R}} p$ if and only if the finite sum in R is idempotent .
- *Exponential* $!(p+q) \sim_{\mathrm{R}} !p|!q$ and $!0 \sim_{\mathrm{R}} 1$ – $!$ is a homomorphism from $+$ to $|$
  $!p \not\sim_{\mathrm{R}} p|!p$ in general (since $!0 \sim_{\mathrm{R}} 0|!0$ implies $0 \sim_{\mathrm{R}} !0 \sim_{\mathrm{R}} 1$).
  For idempotent R, $!p \sim_{\mathrm{R}} 1 + (p|!p)$.

5.2 Sum-of-paths for λ-terms

We illustrate our sum-of-paths interpretation of unidirectional processes by relating to an evaluation semantics of Λ_{R}^{+} terms based on that given in loc. cit. [16] – i.e. we prove *soundness* of the translation given in Section 3.4. We evaluate closed terms of Λ_{R}^{+} to elements of R using a *CEK machine* equipped with an oracle determining which branch is taken at each choice encountered in evaluation. A *state* of the machine is a triple $(C; E; K; w)$ of

[6] It will follow from our full abstraction result that any terms which are not $\sim_{\mathrm{R}}$-equivalent can be separated by pure contexts – i.e. each semiring induces a single notion of equivalence, regardless of which elements are denoted as constants.

$$\frac{}{(\lambda x.M;E;\varepsilon)\Downarrow_{\mathrm{R}} 1} \qquad \frac{(M_i;E;K;w)\Downarrow_{\mathrm{R}} a}{(M_0{+}M_1;E;K;iw)\Downarrow_{\mathrm{R}} a}\, i\in\{0,1\} \qquad \frac{(M;E,(x,N);K;w)\Downarrow_{\mathrm{R}} a}{(\lambda x.M;E;N{::}K;w)\Downarrow_{\mathrm{R}} a}$$

$$\frac{(M;E;N{::}S;w)\Downarrow_{\mathrm{R}} a}{(M\ N;E;K;w)\Downarrow_{\mathrm{R}} a} \qquad \frac{(M;E;K;w)\Downarrow_{\mathrm{R}} b}{(\underline{a}(M);E;K;w)\Downarrow_{\mathrm{R}} a{\cdot}b} \qquad \frac{(M;E,(x,M);K;w)\Downarrow_{\mathrm{R}} a}{(x;E,(x,M);K;w)\Downarrow_{\mathrm{R}} a}$$

Figure 3 Evaluation rules for the Λ^+_{R} CEK machine.

$$\frac{}{(\lambda x.M;\varnothing;\varepsilon;\varepsilon)\Downarrow_{\mathrm{R}} 1} \qquad \frac{(M_i;\mathsf{E};K;w)\Downarrow_{\mathrm{R}} a}{(M_0{+}M_1;\mathsf{E};K;iw)\Downarrow_{\mathrm{R}} a}\, i\in\{0,1\} \qquad \frac{(M;\mathsf{E},(x,N)^j;K;w)\Downarrow_{\mathrm{R}} a}{(\lambda x.M;\mathsf{E};N{::}K;w)\Downarrow_{\mathrm{R}} a}$$

$$\frac{(M;\mathsf{E};N{::}S;w)\Downarrow_{\mathrm{R}} a}{(M\ N;\mathsf{E};K;w)\Downarrow_{\mathrm{R}} a} \qquad \frac{(M;\mathsf{E};K;w)\Downarrow_{\mathrm{R}} b}{(\underline{a}(M);\mathsf{E};K;w)\Downarrow_{\mathrm{R}} a{\cdot}b} \qquad \frac{(M;\mathsf{E},(x,M)^j;K;w)\Downarrow_{\mathrm{R}} a}{(x;\mathsf{E},(x,M)^{j+1};K;w)\Downarrow_{\mathrm{R}} a}$$

Figure 4 Multiset CEK Machine for Λ^+_{R}.

a term C, an *environment* E (a finite set of pairs (x, M) defining a partial function from variables to terms) and a continuation K (a finite list S of terms), and an *oracle* w (an element of the set $\{0,1\}^*$ of binary words). The rules in Figure 3 define a "big-step" reduction relation from states to elements of R.

By induction on derivation, we prove that:

▶ **Lemma 11.** *If $(M; E; K, w) \Downarrow a$ and $(M; E; K; w) \Downarrow a'$ then $a = a'$.*

So for any closed term M we may define the function $\mathsf{ev}_M : \{0,1\}^* \to R$:
$\mathsf{ev}_M(w) = a$ if $(M; \varnothing; \varepsilon; w) \Downarrow_{\mathrm{R}} a$, and $\mathsf{ev}_M(w) = 0$, otherwise.
Hence we may evaluate the sum of paths for M by taking the sum of $\mathsf{ev}_M(w)$ over $\{0,1\}^*$.

To prove soundness of the translation with respect to this operational semantics, we define an equivalent version of the latter in which the environment E is a *finite multiset* of variable bindings (rather than a set), such that application creates a finite (non-deterministically chosen) number of copies of the binding of x to N, invocation of x consumes a single instance and convergence requires that the environment is empty (See Figure 4.) We prove the following lemma by a straightforward induction on derivation ($\mathsf{sup}(\mathsf{E})$ is the *support* of the multiset E):

▶ **Lemma 12.** *$(M; \mathcal{E}; K; w) \Downarrow_R a$ if and only if there exists a multiset E such that $\mathsf{sup}(\mathsf{E}) \subseteq \mathcal{E}$ and $(M; \mathsf{E}; K; w) \Downarrow_R a$.*

▶ **Proposition 13.** *For any closed term M of Λ^+_R, $(\!|M|\!) \Downarrow_R \Sigma_{w\in\{0,1\}^*} \mathsf{ev}_M(w)$.*

Proof. By Lemma 12, it is sufficient to show $(\!|M; \mathsf{E}; K|\!) \Downarrow_{\mathrm{R}} \Sigma_{w\in\{0,1\}^*} \mathsf{ev}(M; \mathsf{E}; K; w)$, where:

- $\mathsf{ev}(M; \mathsf{E}; K; w)$ is the evaluation function for states of the multiset CEK machine – i.e. $\mathsf{ev}(M; \mathsf{E}; K; w) = a$ if $(M; \mathsf{E}; K; w) \Downarrow_{\mathrm{R}} a$, and $\mathsf{ev}(M, \mathsf{E}, K, w) = 0$, otherwise.
- $(\!|M; \mathsf{E}; K|\!)$ is defined by extending the translation of Λ^+_{R}-terms to states of the multiset CEK machine:

$$(\!|M; \{(x_1, N_1)^{j_1}, \dots, (x_k, N_k)^{j_k}\}; P_1 : \dots : P_l|\!) =$$
$$(\!|M|\!)(v_1)|\tfrac{1}{!j_1}|(\overline{x_1}(\underline{y}, -)(\!|N_1|\!)(y))^{j_1}| \dots |\tfrac{1}{!j_k}|(\overline{x_k}(\underline{y}, -)(\!|N_k|\!)(y))^{j_k}|v_1(v_2, \underline{w_1})|(\!|P_1|\!)(w_1)| \dots$$
$$\dots |v_l(u, \underline{w_l})|(\!|P|\!)_l(w_l).$$

This is shown by nested multiset induction on $\ell(\!|M; \mathsf{E}; K; w|\!)$. ◀

6 Soundness and Full Abstraction

We now prove soundness and completeness results relating the operational and denotational semantics of unidirectional terms. We first show that structurally congruent terms have the same denotation, using the symmetric monoidal structure and the properties of the trace operator

▶ **Lemma 14.** *For processes* $\Gamma \vdash; p, q; \Delta$*, if* $p \equiv q$ *then* $[\![\Gamma \vdash p; \Delta]\!]_R = [\![\Gamma \vdash q; \Delta]\!]_R$.

Soundness of the communication rule is established using the differential structure. Given a differential bialgebra (A, B) we may derive a morphism $\varepsilon : A \otimes B \to B = (\xi \otimes B); \mu$ (this corresponds to the *deriving transform* for the differential operation). For $n \geq 0$ let $\delta_A^n : B \to B^{\otimes n}$ be n-fold comultiplication derived from the comonoid structure on B, and for each $i \leq n$, let $\theta_{i,n} : A^{\otimes n} \to A^{\otimes n}$ be the permutation isomorphism swapping the first and ith copies of A. The equations for a differential bialgebra yield: $\varepsilon; \delta_{n+1}; \zeta^{\otimes n+1} : (A \otimes B) \to A^{\otimes n+1} = \Sigma_{i \leq n}(A \otimes (\delta_n; \zeta^{\otimes n})); \theta_{i,n+1}$.

▶ **Lemma 15.** *If* $x \notin FV^-(p)$ *then* $[\![\nu x.\overline{x}(u, v)|x(y_1, z_1)| \ldots |x(y_{n+1}, z_{n+1})|p]\!]$ $= \Sigma_{i \leq n}[\![\nu x.\overline{x}(u, v)|x(y_1, z_1)| \ldots |u = y_i|z_i = v| \ldots |x(y_{n+1}, z_{n+1})|p]\!]$.

Proof. Suppose $\Gamma \vdash p; \Delta, x$, with $x \notin \Gamma$ – so p denotes a morphism $[\![p]\!] : [\![\Gamma]\!] \to [\![\Delta]\!] \otimes B$. Then $\overline{x}(u, v)|p$ denotes (a currying of) $([\![p]\!] \otimes (B \otimes B^*)); ([\![\Delta]\!] \otimes \varepsilon) : [\![\Gamma]\!] \otimes (B \otimes B^*) \to [\![\Delta]\!] \otimes B$, and $x(y_1, z_1)| \ldots |x(y_{n+1}, z_{n+1})$ denotes (an uncurrying of) $\delta_n; \zeta^{\otimes n} : B \to (B \otimes B^*)^n$.

By dinaturality of the trace, $\nu x.\overline{x}(u, v)|x(y_1, z_1)| \ldots |x(y_{n+1}, z_{n+1})|p$ denotes the composition of these morphisms – i.e. $([\![p]\!] \otimes (B \otimes B^*)); ([\![\Delta]\!] \otimes (\varepsilon; \delta_n; \zeta^{\otimes n})) : [\![\Gamma]\!] \otimes (B \otimes B^*) \to \Delta \otimes (B \otimes B^*)^n)$.

By the differential rule above this is equal to $[\![p]\!] \otimes (\Sigma_{i \leq n}(B \otimes B^*) \otimes (\delta_n; \zeta^{\otimes n}); \theta_{i,n+1})$, and hence to $\Sigma_{i \leq n}[\![\nu x.x(y_1, z_1)| \ldots |u = y_i|z_i = v| \ldots |x(y_{n+1}, z_{n+1})|p]\!]$. ◀

Soundness of the evaluation rules for choice and replication follow directly from their definition, and for (non-acyclic) explicit fusion, from the yanking rule for the trace operator. However, the categorical structure is not sufficient to establish that every failure denotes the zero map – this requires a global argument to show that every failure corresponds to "deadlocked" matrix with a trace of zero.

▶ **Lemma 16.** *If* $p \not\Downarrow$ *then* $[\![p]\!] = 0$.

Proof. Suppose $p \not\Downarrow$. Then $p \equiv \nu x_1 \ldots x_m.q$ where q is a parallel composition of solos and constants. By definition, $[\![p]\!]$ is the trace of the $B^m \times B^m$ matrix $[\![x_1, \ldots, x_m \vdash q; x_1, \ldots, x_m]\!]$ – i.e. the sum of the entries on the diagonal of $[\![q]\!]$. Suppose (for a contradiction) that this is non-zero – then there is a non-zero entry on this diagonal – i.e. there exist $e_1, \ldots, e_m \in B$ such that $[\![q]\!](e_1, \ldots, e_m, e_1, \ldots, e_m) \neq 0$.

Choose the smallest $n \in \mathbb{N}$ such that $e_1, \ldots, e_m \in B_{n+1}$. Then (without loss of generality) there exists j such that $q \equiv x_j(y, z)|q'$ and $e_j \notin B_n$. By assumption that p is a failure, x_j must appear as a mobile output name in q' (otherwise, the communication rule may be applied to reduce p to 0). Suppose (w.l.o.g.) $q' \equiv \overline{x_k}(u, x_j)|q''$ for some q''. Then there exists d with $(d, e_j) \in e_k$. But $e_k \in B_{n+1}$, and therefore $e_j \in B_n$, a contradiction. ◀

▶ **Proposition 17.** *For any closed term* p*,* $p \Downarrow_R a$ *if and only if* $[\![p]\!]_R(*, *) = a$.

Proof. From left-to-right, this follows from an induction on $\ell(p)$, using Lemmas 14 15 and 16. For the converse, suppose $[\![p]\!]_R(*, *) = a$. By Proposition 8, $p \Downarrow_R b$ for some b, and by the left-to-right implication just established, $a = b$. ◀

6.1 Full Abstraction

We will now establish a full abstraction result, showing that contextually equivalent R-weighted solo terms denote the same matrix over R – i.e. if $\Gamma \vdash p, q; \Delta$ where $\Gamma \cap \Delta = \varnothing$, $p \sim_{\mathrm{R}} q$ if and only if $[\![p]\!]_{\mathrm{R}} = [\![q]\!]_{\mathrm{R}}$[7]. This establishes the closeness of the syntax and semantics, and also that we can define a testing equivalence for weighted processes which obeys the algebraic laws of R-modules, and differential nets. Note that the R-weighted model of PCF in [16] is not fully abstract, essentially because it contains finite elements which are not denoted by any term. By contrast, we will show thatit is straightforward to define a basis of definable elements for each R-module in our model.

For an element $b \in B$, define $\chi^-_b : B \to I$ and (its transpose) $\chi^+_B : I \to B$:
$\chi^-_b(a, *) = \chi^+_b(*, a) = 1$ if $a = b$: $\chi^-_b(a, *) = \chi^+_b(*, a) = 0$, otherwise.
$\{\chi^-_b \mid b \in B\}$ and $\{\chi^+_b \mid b \in B\}$ are *bases* for the R-modules $\mathsf{Mat}_{\mathrm{R}}(B, I)$ and $\mathsf{Mat}_{\mathrm{R}}(I, B)$.

▶ **Lemma 18.** *For all $b \in B$, there exist terms $x \vdash p^-_b$ and $\vdash p^+_b; y$ which denote χ^-_b and χ^+_b.*

Proof. We prove that if $b \in B_k$ then χ^-_b and χ^+_b are definable, by induction on k. $B_0 = \varnothing$, so suppose $b \in B_{k+1}$. Then b is a finite multiset $\{(b^-_1, b^+_1), \ldots, (b^-_m, b^+_m)\}$, where each $b^-_i, b^+_i \in B_k$. So by hypothesis, for each i, $\chi^-_{b^+_i}$ is definable as a term $u \vdash p^-_i$ and each $\chi^+_{b^-_i}$ as $\vdash p^+_i; v$. Hence χ^-_b is definable as $p^-(x) = x(\underline{v}, \underline{u})p^-_1|p^+_1| \ldots |x(\underline{v}, \underline{u})p^-_m|p^+_m$. By symmetry, χ^+_b is definable as $\_ \vdash p^+(y); y$. ◀

▶ **Theorem 19.** *If $\Gamma \vdash q, q'; \Delta$, where $\Gamma \cap \Delta = \varnothing$ then $[\![q]\!]_R = [\![q']\!]_R \Longleftrightarrow q \sim_R q'$.*

Proof. Equational soundness follows from Proposition 17.

To prove completeness, suppose $x_1, \ldots, x_m \vdash q, q'; y_1, \ldots, y_n$, and $[\![q]\!]_{\mathrm{R}} \neq [\![q']\!]_{\mathrm{R}}$. There exist $b^-_1, \ldots, b^-_m, b^+_1, \ldots, b^+_n \in B$ such that $[\![q]\!](b^-_1, \ldots, b_m, b^+_1, \ldots, b^+_n) \neq [\![q']\!](b^-_1, \ldots, b_m, b^+_1, \ldots, b^+_n)$. By Lemma 18, each $\chi^+_{b^-_i}$ and $\chi^-_{b^+_j}$ are definable as terms $\_ \vdash p^+_i; x_i$ and $y_j \vdash p^-_j$ for $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n\}$.

Let $C[\_] = \nu x_1 \ldots x_m.\nu y_1 \ldots y_n.[\_]|p^+_1| \ldots |p^+_m|p^-_1| \ldots |p^-_n$. By Proposition 17 $C[q] \Downarrow_{\mathrm{R}} [\![q]\!](b^-_1, \ldots, b_m, b^+_1, \ldots, b^+_n)$ and $C[q'] \Downarrow_{\mathrm{R}} [\![q]\!](b^-_1, \ldots, b_m, b^+_1, \ldots, b^+_n)$ – i.e. $q \not\sim_{\mathrm{R}} q'$ as required. ◀

7 Conclusions and Further Directions

We have defined a semantic basis for name mobility which focusses on quantitative testing. Areas in which it might be extended, refined or applied, include:

- Describing systems: which classes of processes can be expressed in the (acyclic part of) the calculus of R-solos? In particular, can we establish a precise relationship with Beffara's quantitative trace semantics of the πI-calculus [2].
- Expressing properties: which quantitative and qualitative properties of systems can be naturally expressed using quantitative solos?
- Computing sums of paths: For which terms can we give algorithms for computing the evaluation function?
- Constructing new models: Are there instances of reflexive differential bialgebras with richer structure, for example in categories of games or event structures?

[7] Our result is restricted to terms with disjoint input and output channels, essentially because input and output capabilities are modelled separately. Without this restriction, full abstraction may fail – e.g. in an idempotent semiring, the term $\nu y.\nu z.x(y, z)|\overline{x}(y, z)$ (which forwards to itself) is observationally equivalent to the unit, 1.

References

1 A. Bahamonde. Tensor product of partially-additive monoids. *Semigroup Forum*, 32(1):31–53, 1985.
2 Emmanuel Beffara. Quantitative testing semantics for non-interleaving. *CoRR*, abs/0906.3994, 2009.
3 G. Bellin and P. J. Scott. On the pi-calculus and linear logic. *Theoretical Computer Science*, 135(1):11–65, 1994.
4 R. F. Blute, J. R. B. Cockett, and R. A. G. Seely. Differential categories. *Mathematical. Structures in Comp. Sci.*, 16, 2006.
5 M. Boreale and F. Gaducci. Processes as formal power series: A coinductive approach to denotational semantics. *Theoretical Computer Science*, 360(1–3):440–458, 2006.
6 N. Dershowitz and Z. Manna. Proving termination with multiset orderings. *Communications of the ACM*, 22:465–476, 1979.
7 T. Ehrhard and O. Laurent. Acyclic solos and differential interaction nets. *Logical Methods in Computer Science*, 6(3), 2010.
8 T. Ehrhard and O. Laurent. Interpreting a finitary pi-calculus in differential nets. *Information and Computation*, 208(6):606–633, 2010.
9 T. Ehrhard and L. Regnier. The differential lambda-calculus. *Theoretical Computer Science*, 309, 2003.
10 T. Ehrhard and L. Regnier. Differential interaction nets. *Theoretical Computer Science*, 364(2):166–195, 2006.
11 C. Fornet and G. Gonthier. The reflexive chemical abstract machine and the join-calculus. In *23rd ACM Symposium on Principles of Programming Languages (POPL'96)*, 1996.
12 J. S. Golan. *The theory of semirings with applications in mathematics and theoretical computer science*. Addison-Wesley, 1992.
13 R. Guitart. Tenseurs et machines. *Cahiers de Topologie et Geometrie Differentielle*, XXI(1):5–62, 1980.
14 K. Honda and N. Yoshida. On reduction-based process semantics. *Theoretical Computer Science*, 152:437–686, 1995.
15 A. Joyal, R. Street, and D. Verity. Traced monoidal categories. *Math. Proc. Camb. Phil. Soc.*, 119:447–468, 1996.
16 J. Laird, G. Manzonetto, G. McCusker, and M. Pagani. Weighted relational models of typed lambda-calculi. In *Proceedings of LICS'13*, 2013.
17 C. Laneve and B. Victor. Solos in concert. *Mathematical Structures in Computer Science*, 13(5), 2003.
18 P. Melliès, N. Tabareau, and C. Tasson. An explicit formula for the free exponential modality of linear logic. In *Proc. ICALP'09*, number 5556 in LNCS, pages 247–260, 2009.
19 R. Milner. Functions as processes. *Math. Struct. in Computer Science*, 2(2):119–141, 1992.
20 Robin Milner, Joachim Parrow, and David Walker. A calculus of mobile processes, part i. *I AND II. INFORMATION AND COMPUTATION*, 100, 1989.
21 M. Mohri. Semiring frameworks and algorithms for shortest-distance problems. *Journal of Automata, Languages and Combinatorics*, 7(3):321–350, 2002.
22 C. Laneve. J. Parrow and B. Victor. Solo diagrams. In *Proceedings of TACS 2001*, LNCS. Springer, 2001.
23 J. Parrow and B. Victor. The fusion calculus: Expressiveness and symmetry in mobile processes. In *Proceedings of LICS'98*, pages 176–185. IEEE press, 1998.
24 D. Sangiorgi and D. Walker. *The Pi-Calculus: A theory of mobile processes*. Cambridge University Press, 2001.
25 L. Wischik and P. Gardner. Explicit fusions. *Theoretical Computer Science*, 340(3):606–630, 2005.