Quantitative testing semantics for non-interleaving

Emmanuel Beffara*

IML, CNRS & Université Aix-Marseille II

April 15, 2009

Abstract. This paper presents a non-interleaving denotational semantics for the π-calculus. The basic idea is to define a notion of test where the outcome is not only whether a given process passes a given test, but also in how many different ways it can pass it. More abstractly, the set of possible outcomes for tests forms a semiring, and the set of process interpretations appears as a module over this semiring, in which basic syntactic constructs are affine operators. This notion of test leads to a trace semantics in which traces are partial orders, in the style of Mazurkiewicz traces, extended with readiness information. Our construction has standard may- and must-testing as special cases.

1 Introduction

The theory of concurrency has developed several very different models for processes, focusing on different aspects of computation. Process calculi are an appealing framework for describing and analyzing concurrent systems, because the formal language approach is well suited to modular reasoning, allowing to study sophisticated systems by means of abstract programming primitives for which powerful theoretical tools can be developed. However, the vast majority of the semantic studies on process calculi like the π-calculus have focused on the so-called interleaving operational semantics, which is the basic definition of the dynamic of a process: the interaction of a program with its environment is reduced to possible sequences of transitions, thus considering that parallel composition of program components is merely an abstraction that represents all possible ways of combining several sequential processes into one.

There is clearly something unsatisfactory in this state of things. Although sophisticated theories have been established for interleaving semantics, most of which are based on various forms of bisimulation, they fundamentally forget the crucial (and obvious) fact that concurrent processes are intended to model situations where some events may occur independently. Attempts at recovering this notion of independence in existing theories have been made, for instance in the form of subtle variations on bisimulation or by fully abstract encodings of non-interleaving semantics into interleaving ones (in particular in Sangiorgi's work on locality and causality [13, 3]). More recently, the old idea of Winskel's interpretation of CCS in event structures [14] has been revisited by Crafa, Varacca and Yoshida to provide an actually non-interleaving operational semantics for the π-calculus, using extensions of event structures [5].

This paper presents an attempt at defining a semantics for the π-calculus that is both non-interleaving (sometimes called "truly concurrent") and denotational, in the sense that the internal dynamics of a process is hidden, and only the part that is observable by other processes is kept.

*Work partially supported by the French ANR project Choco.

These two requirements may seem contradictory: "denotational" as we mean it leads to the definition of testing semantics, which in turn leads to trace semantics, which is very interleaving in nature. Indeed, consider the prototypical case of $a \mid b$ versus $a.b + b.a$: how is it possible to distinguish them when looking at their interactions? Both can do a then b or b then a, but in the first case the paths $a.b$ and $b.a$ are in fact one same run since a and b are independent, while in the second case they correspond to two actually different choices. We solve the contradiction by elaborating on this simple idea: instead of checking whether a given process passes a given test, we check in how many different ways it can pass it. The word "different" here refers to different choices being made in situations of non-determinism, and not simply different orderings of the same actions.

The approach presented here follows previous work by the author [1] on the search for algebraically pleasant denotational semantics of process calculi. The first step was to introduce in the π-calculus an additive structure (a formal sum with zero) that represents pure non-determinism, and this technique proved efficient enough to provide a readiness trace semantics (in the style of Olderog and Hoare [12]) with a complete axiomatization of equivalence for finite terms. The second step presented here further extends the space of processes with arbitrary linear combinations, giving a meaning to these combinations in terms of quantitative testing. This introduction of scalar coefficients was not possible in the interleaving case, because of the combinatorial explosion that arose even when simply composing independent traces; quotienting by homotopy is the proper solution to this problem. Growing the space of processes to get more algebraic structure is motivated by the idea that better structured semantics gives cleaner mathematical foundations for the object of study, in the hope that the obtained theory will be reusable for different purposes and that it will benefit from existing mathematical tools.

Outline. In section 2, we define the calculus on which our study is built: a finite form of the πI-calculus. An non-interleaving operational semantics is defined as follows: transitions are those of the standard calculus, decorated with the position of each action involved in a given transition, so that transitions are independent if they derive from actions at independent positions. Two execution paths are then considered homotopic if they differ only by permutation of independent actions. This technique is a variant of proved transitions introduced by Boudol and Castellani [4] and notably studied by Degano and Priami [6, 7].

In section 3, the notion of test is defined. Outcomes are taken from a semiring $\mathbb{K}$ in which multiplication represents the parallel composition of independent results and addition represents the combination of outcomes from different (non homotopic) runs. Processes are equivalent if they yield the same outcome in all contexts. The space of process equivalence classes appears a $\mathbb{K}$-module, on which the outcome is a linear form, and syntactic constructs are affine operators.

In section 4, we derive a first denotational semantics of processes as linear forms over this space, in a construction similar to that of the theory of distributions. This construction provides an abstract interpretation of recursive processes without having to include them in the initial construction of tests.

In section 5, we further describe the space of finite processes by showing that every finite process is a linear combination of traces. Our notion of trace is an asynchronous variant of the traces induced by standard semantics: they are partially ordered finite sets of actions, augmented with readiness information. This provides a second, more concrete denotational semantics that illustrates the expressiveness of our notion of test.

Finally, in section 6, we show that standard forms of test are particular cases of our construction, obtained by choosing an appropriate semiring for outcomes.

Future and related works. The present work is by no means a complete study of quantitative testing semantics and its possible applications, but rather a presentation of the basic ideas and their consequences. A first objective is to clarify the relationships between the two proposed semantics, possibly by establishing that traces form a basis of the space of processes (maybe by using a ring or field instead of a semiring for outcomes). Another challenging direction for future work is using the linear-algebraic interpretation for specification of processes, using tools like differential equations to specify behaviours; this should provide a reconstruction of the semantics on arbitrary vector spaces instead of the concrete space of processes, which could be a way to a new family of denotational semantics for process calculi.

Along with this long-term ideas, it is naturally interesting to extend our work with more features in the calculus. A more precise account of recursion is a desirable thing: surely infinite behaviours fit in our framework, but the present work does not study it in full detail for lack of space. External choice is a natural feature to add in the framework, but previous work [1] suggests that it is painless. Unrestricted name passing, on the other hand, is a more delicate matter, and we believe that getting a satisfactory understanding of the more regular case of internal mobility first is necessary to handle it.

Several works by other authors are related to the present work. Crafa, Varacca and Yoshida's event structure semantics probably has very strong relationships with our trace semantics: it has to be expected that their event structures can be used as an intermediate between the process calculus and the traces, and that traces and outcomes can be deduced from configurations of the event structures. The operational semantics and its similarity to Mazurkiewicz traces also suggests that relations could be made with more abstract semantics, like Melliès and Mimram's asynchronous games [10, 11]. Previous work on the search for algebraic semantics of processes include Boreale and Gadducci's processes as formal series [2], which has notable similarities with the present work, although their work is carried out in CSP. Finally, strong relationships are expected with differential interaction nets [9, 8], which have linear algebraic semantics and are expressive enough to encode the π-calculus.

Note. Many technical proofs were moved out to the appendix and replaced by sketches, for lack of space and in the interest of readability.

2 Parallel operational semantics

We consider the π-calculus with internal mobility, or πI-calculus, extended with a parallel composition without interaction and with *outcomes* from a commutative semiring $\mathbb{K}$. We consider the monadic variant of the calculus for simplicity, but using the polyadic form would not pose any significant problem. The most important point is that we consider finite processes, without recursion, for the construction of our framework, and we handle potentially infinite behaviours in a second phase in section 4.

Definition 1. We assume a countable set $\boldsymbol{N}$ of names. Polarities are elements of $\boldsymbol{P} = \{\downarrow, \uparrow\}$. Terms are generated by the following grammar:

$$\begin{array}{lrll}
\text{actions} & \alpha := & u^{\varepsilon}(x) & \text{with } u, x \in \boldsymbol{N} \text{ and } \varepsilon \in \boldsymbol{P} \\
\text{processes} & P, Q := & k & \text{outcome, with } k \in \mathbb{K} \\
 & & \alpha.P & \text{action} \\
 & & \_P & \text{performed action} \\
 & & P \mid Q & \text{parallel composition with interaction} \\
 & & P \parallel Q & \text{parallel composition without interaction} \\
 & & (\boldsymbol{\nu} x)P & \text{hiding}
\end{array}$$

$$\frac{}{\alpha.P \xrightarrow{\alpha:\varepsilon} \_P} \qquad \frac{P \xrightarrow{a} P'}{\_P \xrightarrow{1.a} \_P'} \qquad \frac{P \xrightarrow{u^{\varepsilon}(x):\iota} P' \qquad Q \xrightarrow{u^{\neg\varepsilon}(y):\kappa} Q'}{P \mid Q \xrightarrow{(1.\iota,2.\kappa)} (\boldsymbol{\nu}x)(P' \mid Q'[x/y])} \qquad \frac{P \xrightarrow{a} P' \qquad x \notin a}{(\boldsymbol{\nu}x)P \xrightarrow{a} (\boldsymbol{\nu}x)P'}$$

$$\frac{P \xrightarrow{a} P'}{P \mid Q \xrightarrow{1.a} P' \mid Q} \qquad \frac{P \xrightarrow{a} P'}{Q \mid P \xrightarrow{2.a} Q \mid P'} \qquad \frac{P \xrightarrow{a} P'}{P \parallel Q \xrightarrow{1.a} P' \parallel Q} \qquad \frac{P \xrightarrow{a} P'}{Q \parallel P \xrightarrow{2.a} Q \parallel P'}$$

Table 1: Transition rules

Terms are considered up to renaming of bound names and commutation of restrictions, i.e. $(\boldsymbol{\nu}x)(\boldsymbol{\nu}y)P = (\boldsymbol{\nu}y)(\boldsymbol{\nu}x)P$, with the standard convention that all bound names are distinct from all other names.

The parallel composition without interaction allows us to write a term like $a \parallel \bar{a}$ which can perform the dual actions a and $\bar{a}$ independently but does not allow them to synchronize — this slightly extends the expressiveness of the calculus but not in a dramatic way, and it simplifies the theory.

The prefix _ represents an action that already occurred. It has no computational meaning but has the effect that the positions of actions in the terms are preserved when reducing, which will simplify definitions below.

We want to define an operational semantics in which commutation of independent transitions is allowed. In order to make this possible by only looking at transition labels, we have to enrich the labels so that different occurrences of a given action are distinguishable. We do this by simply introducing in each label the positions in the syntax tree of all actions involved (as a consequence, the operational semantics cannot be defined up to structural congruence).

Definition 2. A position is a finite sequence of integers. The concatenation of ι and κ is written $\iota.\kappa$, the empty position is written ε. The prefix order is written $\leqslant$ and two positions ι and κ are independent (written $\iota \mathbin{/\!\!/} \kappa$) if they are incomparable.

Definition 3. Transition labels can be of one of two kinds:

$$\begin{array}{rll} a, b := & u^{\varepsilon}(x) : \iota & \text{visible action} \\ & (\iota, \kappa) & \text{internal transition} \end{array}$$

For a label a and a position ι, $\iota.a$ denotes the label a where each position κ is replaced with $\iota.\kappa$. Transitions are derived by the rules of table 1.

An interaction is finite sequence of transition labels. A path is a finite sequence of internal transition labels. An interaction $p = a_1 a_2 \dots a_n$ is valid for P, written $p \in P$, if there are valid transitions $P \xrightarrow{a_1} P_1 \xrightarrow{a_2} \cdots \xrightarrow{a_n} P_n$.

This technique can be seen as a version of Boudol and Castellani's proved transitions [4, 7] simplified for our purpose. It is clear that for all term P and interaction $p \in P$, there is exactly one term P/p such that there is a transition sequence $P \xrightarrow{p} P/p$ (up to renaming of revealed bound names). Remark that by removing all positions from labels (replacing (ι, κ) by τ) one gets the standard labeled transition system for the πI-calculus.

Definition 4. Two labels a and b are independent (written $a \mathbin{/\!\!/} b$) if all positions in a are independent of all positions in b. Homotopy is the smallest congruence $\approx$ over paths such that $ab \approx ba$ when $a \mathbin{/\!\!/} b$.

Two execution paths of a given term are homotopic if it is possible to transform one into the other by exchanging consecutive transitions if they are independent. Prefixing generates local constraints which propagate to paths by this relation. A first remark is that transition labels contain enough information so that homotopy does not depend on the term in which paths are taken.

Proposition 1. *For all term P and all interactions p, q such that $p \approx q$, $p \in P$ if and only if $q \in P$, and then $P/p = P/q$.*

sketch. The basic ingredient is that if $ab \in P$ and $a \mathbin{/\!/} b$, then a and b involve actions in different parts of the term P, therefore none of them prefixing any other. By a simple case analysis one checks that the transitions can be swapped, so $ba \in P$. The fact that $P/ab = P/ba$ is also easily checked, the only subtle case is that of two consecutive interactions in a term $P \mid Q$ that introduce hidings in different orders, this is where we use the fact that terms are considered up to permutation of hidings. □

Definition 5. A pre-trace is a homotopy class of interactions. A run is a homotopy class of maximal paths. The sets of pre-traces and runs of a term P are written $\mathcal{P}(P)$ and $\mathcal{R}(P)$ respectively. The unique reduct of a term P by a pre-trace ρ is written P/ρ.

Runs are the intended operational semantics: they are complete executions of a given system, forgetting unimportant interleaving of actions and remembering only actual ordering constraints. A pre-trace can be seen as a Mazurkiewicz trace on the infinite language of transition labels, with the independence relation from definition 4, except that, because of our transition rules (and because of the use of the place-holder $\_$), each label occurs at most once in any interaction. A crucial fact is that pre-traces are uniquely defined by the set of their labels:

Proposition 2. *Let p and q be two interactions of a term P such that p and q are permutations of each other, then $p \approx q$.*

Proof. We first prove that for all interaction $a_1 \dots a_n b \in P$ such that $b \in P$ we have $a_1 \dots a_n b \approx b a_1 \dots a_n$, by induction on n. The case $n = 0$ is trivial. For the case $n \geqslant 1$, remark that the hypothesis implies $a_1 \mathbin{/\!/} b$: if some position in a_1 was less than a position in b then b could only occur after a_1, which contradicts $b \in P$, and $a_1 \in P$ also implies that no position in b is less than a position in a. Therefore we have $ba_1 \in P$ and $ba_1 \approx a_1 b$. Applying the induction hypothesis on P/a_1 yields $ba_2 \dots a_n \approx a_2 \dots a_n b$ from which we conclude. The case of arbitrary permutations follows by recurrence on the length of p and q. □

Definition 6. Let P be a term and $\rho \in \mathcal{P}(P)$. By proposition 2, ρ is identified with the set of its labels. The causal order in ρ is the partial order $\leqslant_\rho$ on labels in ρ such that $a \leqslant_\rho b$ if $a = b$ or a occurs before b in all interactions in ρ.

This presentation is much simpler to handle than explicit sets of runs, so this is the one we will mainly use. Interactions that constitute a given pre-trace are simply the topological orderings of this partially ordered set of transitions. Traces are a further quotient of pre-traces, defined and studied in section 5.

3 Quantitative testing

We now define a form of observation based on interaction, in the style of testing equivalences, that takes homotopy into account. Standard testing naturally leads to interleaving semantics, so we have to refine our notion of test, and that is what outcomes are for. The set $\mathbb{K}$ is a semiring in order to represent two ways of combining results: the product is the parallel composition of independent results and the sum is the combination of results from distinct runs.

commutativity	$P \mid Q \simeq Q \mid P$	$P \parallel Q \simeq Q \parallel P$
associativity	$(P \mid Q) \mid R \simeq P \mid (Q \mid R)$	$(P \parallel Q) \parallel R \simeq P \parallel (Q \parallel R)$
neutrality	$P \mid 1 \simeq P$	$P \parallel 1 \simeq P$
scope commutation	$(\boldsymbol{\nu}x)(\boldsymbol{\nu}y)P \simeq (\boldsymbol{\nu}y)(\boldsymbol{\nu}x)P$	
scope extrusion	$(\boldsymbol{\nu}x)(P \mid Q) \simeq P \mid (\boldsymbol{\nu}x)Q$	with $x \notin \mathrm{fn}(P)$
scope neutrality	$(\boldsymbol{\nu}x)k \simeq k$	
non-interaction	$(P \parallel Q) \mid R \simeq (P \mid R) \parallel Q$	with $\mathrm{fn}(Q) \cap \mathrm{fn}(R) = \emptyset$
place-holder	$\_P \simeq P$	
inaction	$(\boldsymbol{\nu}u)u^{\varepsilon}(x).P \simeq 1$	
non-interference	$(\boldsymbol{\nu}u)(u(x).P \mid \bar{u}(x).Q) \simeq (\boldsymbol{\nu}ux)(P \mid Q)$	

Table 2: Basic equivalences.

Definition 7. The state $s(P) \in \mathbb{K}$ of a term P is the product of all outcomes in active position in P:

$$s(k) := k, \quad s(\alpha.P) := 1, \quad s(\_P) := s((\boldsymbol{\nu}x)P) := s(P), \quad s(P \mid Q) := s(P \parallel Q) := s(P)\, s(Q).$$

The outcome of a term P is $\langle P \rangle = \sum_{\rho \in \mathcal{R}(P)} s(P/\rho)$. Two terms P and Q are observationally equivalent, written $P \simeq Q$, if $\langle P \mid R \rangle = \langle Q \mid R \rangle$ for all R.

Classic forms of test intuitively correspond to the case where $\mathbb{K}$ is the set of booleans for the two outcomes success and failure, with operations defined appropriately. This particular case is detailed in section 6.

Theorem 1. *Observational equivalence is a congruence.*

sketch. This proof is quite technical. For the action prefix, the basic argument is to partition the runs of $\alpha.P \mid R$ into those that trigger α and those that do not. The latter are the same in $\alpha.Q \mid R$. The former are further split into one class for each way that R can trigger α, i.e. for each occurrence of $\bar{\alpha}$ in R and each way of reaching it. The contribution of each class to the outcome of $\alpha.P \mid R$ has the form $\langle P \mid R' \rangle$, which allows us to equate it with $\langle Q \mid R' \rangle$ and get back the equality $\langle \alpha.P \mid R \rangle = \langle \alpha.Q \mid R \rangle$.

The case of composition with interaction relies on the easily proved associativity $\langle (P \mid R) \mid S \rangle = \langle P \mid (R \mid S) \rangle$. The case of composition without interaction is more subtle, it is proved using a rewriting of the test $\langle (P \parallel R) \mid S \rangle$ into a sum of tests of the form $\langle (P \mid R') \mid S' \rangle$ in which non-interference between P and R' is guaranteed by the disjointness of their free names. The terms R' and S' are mostly R and S with some actions renamed, so as to ensure which interactions are between P and S and which interactions are between R and S. Details of this technique can be found in appendix. □

Proposition 3. *The equivalences of table 2 hold.*

sketch. All the equations are easily proved by establishing bijections between runs of one member and runs of the other. These bijections simply reflect the change in the positions of actions in the terms. For the non-interaction rule, we use the fact that, in the πI-calculus, two terms may interact only if they share some public name. □

Commutative monoid for $\oplus, 0$:

$$P \oplus Q \simeq Q \oplus P \qquad (P \oplus Q) \oplus R \simeq P \oplus (Q \oplus R) \qquad P \oplus 0 \simeq P$$

Action of the semi-ring $\mathbb{K}$:

$$\begin{array}{lll} 1 \cdot P \simeq P & k_1 k_2 \cdot P \simeq k_1 \cdot k_2 \cdot P & \\ 0 \cdot P \simeq 0 & (k_1 + k_2) \cdot P \simeq k_1 \cdot P \oplus k_2 \cdot P & k \cdot (P \oplus Q) \simeq k \cdot P \oplus k \cdot Q \end{array}$$

Bilinearity of compositions, linearity of hiding:

$$\begin{array}{rr} P \mid (Q \oplus R) \simeq (P \mid Q) \oplus (P \mid R) & P \mid (k \cdot Q) \simeq k \cdot (P \mid Q) \\ P \parallel (Q \oplus R) \simeq (P \parallel Q) \oplus (P \parallel R) & P \parallel (k \cdot Q) \simeq k \cdot (P \parallel Q) \\ (\boldsymbol{\nu} x)(P \oplus Q) \simeq (\boldsymbol{\nu} x)P \oplus (\boldsymbol{\nu} x)Q & (\boldsymbol{\nu} x)(k \cdot P) \simeq k \cdot (\boldsymbol{\nu} x)P \end{array}$$

Table 3: $\mathbb{K}$-module laws over processes.

The non-interaction rule is formulated as it is for generality. Note that it implies the intuitive fact that the two compositions coincide for terms with disjoint free names: if $\mathrm{fn}(P) \cap \mathrm{fn}(Q) = \emptyset$ then

$$P \mid Q \simeq (1 \parallel P) \mid Q \simeq (1 \mid Q) \parallel P \simeq Q \parallel P \simeq P \parallel Q.$$

Thanks to these properties, when considering processes up to observational equivalence, we can consider the compositions to be associative and commutative. In this case we use the notation $\prod_{i \in I} P_i$ to denote the parallel composition without interaction of the P_i in any order (assuming only that I is finite).

In order to study processes up to observational equivalence, we will now describe some of the structure of the space of equivalence classes. The first ingredient is to identify an additive structure that represents pure non-determinism.

Proposition 4. *Let $\Pi_{\mathbb{K}}$ be the set of equivalence classes of processes over the semiring of outcomes $\mathbb{K}$. For all terms P and Q and all outcome k, define*

$$\begin{aligned} P \oplus Q &:= (\boldsymbol{\nu} u)((u.P \mid u.Q) \mid \bar{u}.1) \quad \textit{where } u \textit{ is a fresh name}, \\ k \cdot P &:= k \mid P \end{aligned}$$

Then $(\Pi_{\mathbb{K}}, \oplus, 0, \cdot)$ is a $\mathbb{K}$-module, parallel compositions are bilinear operators and hiding is linear, i.e. the equivalences of table 3 hold.

sketch. The proofs reduce to the equation $\langle (P \oplus Q) \mid R \rangle = \langle P \mid R \rangle + \langle Q \mid R \rangle$, which implies all required rules with the equations of table 2. Note that, contrary to the traditional notation, 0 is the outcome zero, which not the neutral element of parallel composition but an absorbing one, neutral for the sum; the usual inactive process is 1. □

Remark that all syntactic constructions on terms induce linear constructions on equivalence classes, except for the action prefix, which is not linear but actually affine. Indeed, for an action α, the term $\alpha.0$ is not equivalent to 0: it will be neutral in executions that do not trigger α, and multiply the outcome by 0 (thus annihilating it) in runs that do. It can be understood as a statement "I could have performed α but I will not do it" so that any run that contradicts this statement has outcome 0. The purely linear part of actions is the opposite: the linear action

Linearity:

$$\hat{\alpha}.(P \oplus Q) \simeq \hat{\alpha}.P \oplus \hat{\alpha}.Q \qquad \hat{\alpha}.(k \cdot P) \simeq k \cdot \hat{\alpha}.P \qquad (\boldsymbol{\nu} u)\hat{u}^{\varepsilon}(x).P \simeq 0$$

Composition of inactions (the subject of β is not bound by α):

$$\begin{array}{ccc} \hat{\alpha}.(\beta.0 \mid P) \simeq \beta.0 \mid \hat{\alpha}.P & \alpha.0 \mid \alpha.0 \simeq \alpha.0 & \alpha.0 \mid \bar{\alpha}.0 \simeq 0 \\ \hat{\alpha}.(\beta.0 \parallel P) \simeq \beta.0 \parallel \hat{\alpha}.P & \alpha.0 \parallel \alpha.0 \simeq \alpha.0 & \end{array}$$

Table 4: Laws of linear actions and inactions.

$\hat{\alpha}.P$ will act as $\alpha.P$ if its environment actually triggers the action, but will turn to 0 if it is never activated.

Definition 8. For all action α and term P, the linear action of α on P is

$$\hat{\alpha}.P := (\boldsymbol{\nu} w)(\alpha.(P \mid w.1) \mid (w.0 \mid \bar{w}.1)) \quad \text{where } w \text{ is a fresh name.}$$

An interaction is said to trigger the linear action if it triggers the action $w.1$. Terms of the form $\alpha.0$ are called an inactions.

This definition has the expected behaviour because of the maximality of runs. If $\hat{\alpha}.P$ is in active position, then any run that does not trigger α must instead trigger $w.0$, hence any such run has outcome 0. A run in which the term $\hat{\alpha}.P$ does not produce 0 must activate α, so that $w.1$ acts instead of $w.0$.

Proposition 5. *For all α and P, $\alpha.P \simeq \hat{\alpha}.P \oplus \alpha.0$. The function $P \mapsto \hat{\alpha}.P$ is linear and the equivalences of table 4 hold.*

sketch. All these equations are proved in similar ways, using the maximality of runs. In any run, if a linear action $\hat{\alpha}.P = (\boldsymbol{\nu} w)(\alpha.(P \mid w.1) \mid (w.0 \mid \bar{w}.1))$ is in active position, either $w.1$ is eventually triggered, which guarantees that α has been triggered and P has reached an active position, or the action $w.0$ must be triggered, which puts the outcome 0 in active position, thus turning the outcome of the run to 0. As a consequence, the only relevant runs are those that do trigger linear actions. As a consequence, in $\hat{\alpha}.(P \oplus Q)$, all relevant runs put the choice $P \oplus Q$ in active position, so the choice must be made between P and Q. For the computation of final results, the precise position of this choice does not matter, only the fact that a choice is made matters, hence the distribution of $\hat{\alpha}$ over choice. The rules for inactions are proved by the similar argument that the only relevant runs are those that do not trigger an inaction. □

Definition 9. A term is *simple* if it is generated by the grammar

$$P, Q := 1,\ \alpha.0,\ \hat{\alpha}.P,\ (P \mid Q),\ (P \parallel Q),\ (\boldsymbol{\nu} x)P$$

An pre-trace $\rho \in \mathcal{P}(P)$ is exhaustive if it triggers all linear actions and no inaction, and no sub-term of P/ρ has the form $Q \mid R$ with Q containing some $\alpha.0$ and R containing $\bar{\alpha}.0$. The set of such pre-traces is written $\mathcal{P}_e(P)$.

Simple terms have the property that the outcome of any run is either 1 or 0. More precisely, it is easy to see that the outcome of a run is 1 if and only if it triggers all linear actions and no inaction. The notion of exhaustive pre-trace is the correct extension of this notion to pre-traces, indeed every run of a simple term $P \mid Q$ with outcome 1 is made of an exhaustive pre-trace of

P and an exhaustive pre-trace of Q. The condition on P/ρ simply rules out interactions of P that lead to a term P' where there are dual inactions that may interact, since that would imply $P' \simeq 0$, as a generalization of the equation $\alpha.0 \mid \bar{\alpha}.0 \simeq 0$.

Remark that, by the decomposition of proposition 5 and the linearity of all constructions of simple terms, we immediately prove that every term is equivalent to a linear combination of simple terms. As a consequence, two terms P and Q are equivalent if and only if for all *simple* term R, $\langle P \mid R\rangle = \langle Q \mid R\rangle$.

4 A linear algebraic semantics

The equivalence of finite processes is defined by the fact that they give the same outcome when tested against the same finite processes. The equivalence class of a term P is thus completely defined by the function $Q \mapsto \langle P \mid Q\rangle$, which can be considered as a function from equivalence classes to outcomes. Moreover, by the properties of the space of processes, we know that this function is linear.

Definition 10. A behaviour is a linear form over $\Pi_{\mathbb{K}}$. A partial behaviour is a linear form defined over a submodule of $\Pi_{\mathbb{K}}$. The behaviour of a term P is the form $[\![P]\!]$ such that, for all $Q \in \Pi_{\mathbb{K}}$, $[\![P]\!](Q) = \langle P \mid Q\rangle$.

Switching from a space to its dual makes the space of considered objects grow, as we will see below. In our context, it allows us to move from inductive objects (finite processes) to coinductive objects (intuitively, this includes infinite terms). This technique is in some sense analogous to the basic idea of the theory of distributions: consider a generalized function as a linear form over simple well-behaved objects (smooth test functions, as analogous of our finite terms).

We now describe a way of giving semantics to infinitary processes, showing that recursive process definitions have solutions as partial behaviours.

Definition 11. We assume we have a set $\boldsymbol{I}$ of process indeterminates of the form $X\langle x_1 \dots x_n\rangle$, which represent an unknown term with free names $x_1 \dots x_n$. The set of partial terms is generated by the same grammar as finite processes (as of definition 1), augmented with indeterminates. The set of indeterminates of a partial term P is written $\operatorname{ind}(P)$.

The refinement preorder is the relation $\sqsubseteq$ over partial terms such that $P \sqsubseteq Q$ if Q is obtained from P by substituting each indeterminate by an arbitrary term with the same free names. The relation $\sqsubseteq_f$ is its restriction to the case when the right-hand side is a finite term.

Definition 12. Let P be a partial term. If there is a $k \in \mathbb{K}$ such that $\langle Q\rangle = k$ for all finite Q with $P \sqsubseteq_f Q$, then we set $\langle P\rangle = k$, otherwise $\langle P\rangle$ is undefined. The interpretation $[\![P]\!]$ is the partial function $Q \mapsto \langle P \mid Q\rangle$ from $\Pi_{\mathbb{K}}$ to $\mathbb{K}$. Two partial terms are equivalent if the have the same interpretation.

This is clearly an extension of the semantics of total terms, since the set of refinements of a total term P is $\{P\}$. One easily checks that this definition of the interpretation of partial terms enjoys the same properties as finite terms:

Proposition 6. *For all partial term P, $[\![P]\!]$ is a partial behaviour. The equations of tables 2 and 3 hold for partial terms. Interpretations are preserved by injective renaming of indeterminates. Equivalence is preserved by prefixing, hiding and composition with partial terms with distinct indeterminates.*

Definition 13. An ideal is a non-empty set A of partial terms that is downwards closed and such that for all $P, Q \in A$ there is an $R \in A$ such that $P \sqsubseteq R$ and $Q \sqsubseteq R$. The interpretation of an ideal A is the upper limit of the interpretations of its elements, that is the partial function $[\![A]\!]$ such that for all P, $[\![A]\!](P) = k$ if $[\![Q]\!](P) = k$ for some $Q \in A$.

The definition of $[\![A]\!]$ is valid since interpretation of partial terms is clearly increasing, when ordering partial terms by refinements and partial functions by extension (or graph inclusion). Note that for all total term P, the set $\{ Q \mid Q \sqsubseteq_f P \}$ is an ideal that has the same interpretation as P.

The set of ideals, ordered by inclusion, is not well founded: if $(x_n)_{n\in\mathbb{N}}$ is an infinite family of names, then each set $A_n = \{ X\langle x_1, \dots, x_i\rangle \mid i \geqslant n \}$ is an ideal and $\{ A_n \mid n \in \mathbb{N} \}$ is an infinite descending chain. However, if we restrict to a finite number of public names (which does not change expressiveness, since bound names are not restricted), then the set is well-founded, and the smallest ideal is the set Ω of all indeterminates with the set of all free names.

Every syntactic construction for total terms naturally induces a construction for ideals, for instance the parallel composition $A \,|\, B$ is the downwards closure is $\{ P \mid Q \mid P \in A, Q \in B \}$ for P and Q chosen with disjoint indeterminates. All these constructions are increasing for inclusion. Moreover, the union of a directed set of ideals is an ideal, so every equation $X = A(X)$ has a solution in ideals (the least fixed point of $X \mapsto A(X)$, i.e. the union of the $A^n(\Omega)$). Consequently, all processes definable by recursion are interpreted by partial behaviours.

5 Asynchronous traces

Simple terms remove one source of ambiguity in the meaning of processes: the fact that each action may or may not be activated. By linearity, they also reduce the computation of outcomes to the computation of the number of non-zero outcomes. However, they do not form a basis of observable process behaviours, because they may contain internal transitions, which are not observable and can be a source of non-determinism.

A trace as defined below can be seen as a deterministic simple term, up to observational equivalence. It has visible actions, with a partial order imposed by some internal prefixing structure, and these actions may not interact with each other, only with the environment; it also contains inactions, representing the fact that the choice was made not to do some of the actions.

Definition 14. A trace T is a tuple $(|T|, p, s, \leqslant, N)$ where

- $|T|$ is a finite set (the events, or action occurrences),
- p is a function from $|T|$ to $\boldsymbol{P}$ (the polarity),
- s is a function from $|T|$ to $\boldsymbol{N} \uplus |T|$ (the subject),
- $\leqslant$ is a partial order over $|T|$ such that $\forall a, b \in |T|$, if $s(b) = a$ then $a < b$,
- N is a finite subset of $\boldsymbol{P} \times (\boldsymbol{N} \uplus |T|)$ (the inactions).

For an action $a \in |T|$, $s(a)$ is the subject of action a, that is the channel on which a happens: if $s(a) \in \boldsymbol{N}$ then it is a public channel, otherwise it is the private channel bound by the action $s(a)$. The set N indicates which actions could have been performed (in parallel) after the trace has been consumed.

Definition 15. Let P be a simple term and let ρ be an exhaustive pre-trace of P. The trace induced by ρ is the trace ρ^* such that

- $|\rho^*|$ is the set of visible transition labels in ρ,
- p maps labels to their polarity,
- s maps labels to their subject, either the name for public channels or the action that creates the name for private channels,
- $\leqslant$ is the causal order (as of definition 6) restricted to visible transition labels,
- N is the set of all (ε, u) such that $u^\varepsilon.0$ occurs in active position in P/ρ.

Note that the condition that $s(b) = a$ implies $a < b$ is satisfied by ρ^*, because in our language the action prefixes are synchronous: in an action $u(x).P$, the action $u(x)$ that binds x is automatically a prefix of all actions on x. However, synchrony is not necessary for this property to hold:, the fact that the name is bound is the important point: even if internal transitions can occur on a bound name, visible transition are possible only after the name has been revealed by the action it is bound to.

The definition above identifies the trace that is the observable content of a pre-trace. With some coding, we can prove that any trace can be implemented in the calculus, in the sense that for every trace T there is a term $\{T\}$ that has a unique exhaustive pre-trace ρ, the content of which is T.

Definition 16. Let T be a trace. For all a and b in $|T|$, let x_{ab}, y_{ab}, z_a be fresh names. For all $a \in |T|$, let $\operatorname{act}(a) = s(a)^{p(a)}(z_a)$ if $s(a) \in \boldsymbol{N}$ and $\operatorname{act}(a) = z_{s(a)}^{p(a)}(z_a)$ if $s(a) \in |T|$ and define

$$A^T_a := \{\hat{x}_{ba}\}_{b<a}.\hat{\operatorname{act}}(a).\Big(\textstyle\prod_{a<c} \hat{\bar{y}}_{ac} \;\Big\|\; \prod_{s(c)=a} A^T_c \;\Big\|\; \prod_{(\varepsilon,a)\in N} z^\varepsilon_a.0\Big)$$

where $\{\hat{x}_{ba}\}_{b<a}$ represents a sequence of prefixes that contains all actions $\hat{x}_{ba}$ for all $b < a$, in any order. The implementation of T is the process

$$\{T\} := (\boldsymbol{\nu} x_{ab} y_{ab})_{a,b\in|T|}\Big(\textstyle\prod_{s(a)\in\boldsymbol{N}} A^T_a \;\Big|\; \prod_{a<b} \hat{y}_{ab}.\hat{\bar{x}}_{ab}\Big) \parallel \prod_{(\varepsilon,u)\in N,\, u\in\boldsymbol{N}} u^\varepsilon.0$$

The intuition is the following: each action in T is translated by the linear action it describes, which provides the right set of visible actions. Inactions are translated straightforwardly. The ordering is imposed by communication on internal names: for each action a, the translation $\hat{\operatorname{act}}(a)$ is prefixed by a blocking input x_{ba} for each action $b < a$. Activating this action frees the signals x_{ac} for all $c > a$, which guarantees that the order is respected. We cannot implement this system one set of names x_{ab}, because the actions $\hat{\operatorname{act}}(a)$ must be composed without interaction, in order to avoid internal transitions between actions that are supposed to implement visible transitions. We thus split each signal into two names, x_{ab} and y_{ab}, and put in parallel (with interaction) a set of forwarders $y_{ab}.\bar{x}_{ab}$ that performs the synchronization between signals. If the subject of an action a is the bound name of an action b, then $\operatorname{act}(a)$ is put in the continuation of action $\operatorname{act}(b)$, which imposes an order between this action; this is compatible with the constraint $b < a$ from the definition of traces. The formal proof (present in the appendix) of the following proposition is based on this intuition.

Proposition 7. *For all trace T, the term $\{T\}$ is simple, has a unique exhaustive pre-trace ρ and $\rho^* = T$.*

This result justifies that $\{T\}$ is considered as an implementation of T. The proposition below proves that traces are actually the part of interactions that are observable by interaction.

Proposition 8. *For all simple term P, $P \simeq \bigoplus_{\rho \in \mathcal{P}_e(P)} \{\rho^*\}$.*

sketch. The idea is that, given a simple process Q, a run $\vartheta \in \mathcal{R}(P \mid Q)$ has a projection ϑ^1 on P that is an exhaustive pre-trace of P. We can then partition $\mathcal{R}(P \mid Q)$ into one class for each exhaustive pre-trace ρ of P and show that the sum of the outcomes of the runs of this class is precisely $\langle \{\rho^*\} \mid Q \rangle$. □

We can thus consider traces as terms of the language. Indeed, given a trace T, all simple terms that have a unique exhaustive pre-trace ρ with $\rho^* = T$ are equivalent to $\{T\}$. When precise syntactic information is needed, T used as a term is a short-hand for $\{T\}$.

Theorem 2. *Every term is equivalent to a linear combination of traces.*

Proof. By the decomposition of affine actions from proposition 5 we get that every term is equivalent to a linear combination of simple terms. By proposition 8, each simple term is in turn equivalent to a sum of trace implementations. The composition of these equivalences, with the module structure of $\Pi_{\mathbb{K}}$, yields a decomposition of every term as a linear combination of trace implementations. □

We can thus define a semantics of processes based on traces, as of definition 14, by reformulating the various constructions for combinations of traces. As an example we give a reformulation of testing for traces. In the definition below, for two traces T and U, if f is a function from $|T|$ to $|U|$, then f is implicitly extended to a function from $|T| \uplus \boldsymbol{N}$ to $|U| \uplus \boldsymbol{N}$ as the identity over names.

Proposition 9. *Let T and U be two traces, $\langle T \mid U \rangle$ is the number of synchronizations of T and U, that is bijections σ from $|T|$ to $|U|$ such that*

- *for all $a \in |T|$, $p_U(\sigma(a)) = \neg p_T(a)$ and $s_U(\sigma(a)) = \sigma(s_T(a))$,*
- *the relation $\{ (a, b) \mid a \leqslant_T b \text{ or } \sigma(a) \leqslant_U \sigma(b) \}$ is acyclic,*
- *for all $(\varepsilon, x) \in N_T$, $(\neg\varepsilon, \sigma(x)) \notin N_U$.*

Proof. Since trace implementations are simple terms, the outcome of a run of $T \mid U$ is always 0 or 1, so $\langle T \mid U \rangle$ is the number of runs with non zero outcomes. As remarked earlier, such runs are always made of exhaustive pre-traces of T and U, and by construction these terms have only one exhaustive pre-trace so relevant runs are completely defined by a bijection between actions of T and actions of U. It is easy to check that the conditions on this bijection are exactly those that define synchronizations. □

We will not develop the trace semantics further here for lack of space, but the abstract reformulation of outcomes above gives an idea of the construction: a finite process is interpreted as a linear combination of traces and all basic operations are defined independently of the semiring $\mathbb{K}$. The linear action prefix maps traces to traces, inactions are basic traces, composition without interaction is a disjoint union of traces, composition with interaction maps a pair of traces to a combination of traces with integer coefficients, hiding $(\boldsymbol{\nu} u)$ maps traces that contain an action on u to 0, and remove inactions on u from other traces.

may and must				may testing				must testing			
$\cdot$	0	1	ω	$+$	0	1	ω	$+$	0	1	ω
0	0	0	0	0	0	1	ω	0	0	1	ω
1	0	1	ω	1	1	1	ω	1	1	1	1
ω	0	ω	ω	ω	ω	ω	ω	ω	ω	1	ω

Table 5: Observation semirings for may and must testing.

6 Classic forms of test

By choosing appropriate structures for $\mathbb{K}$, we can recover the standard may and must testing. In both cases we have $\mathbb{K} = \{0, 1, \omega\}$, where ω represents success. Table 5 show the rules for addition and multiplication for may and must. Using this definition it is clear that P and Q are equivalent for may or must testing if and only if, for all R, $\langle P \mid R\rangle = \omega$ if and only if $\langle Q \mid R\rangle = \omega$. Taking for $\mathbb{K}$ the minimal semiring $\{0, 1\}$ with $1 + 1 = 1$ gives the framework studied by the author in a previous work [1], which also leads to must testing semantics.

These semirings share an important property, namely that all elements are idempotent for addition. This is an important restriction, in particular it implies that summing outcomes cannot count the number of successes or failures. In other words, the "quantitative" part of our testing semantics disappears. We can remark that this constraint imposes to forget non-interleaving, since it allows us to decompose everything as totally ordered traces.

Theorem 3. *If $\forall x, x + x = x$, then $\Pi_{\mathbb{K}}$ is generated by totally ordered traces.*

Proof. We prove the equivalent fact that each trace is equivalent to the sum of all its total orderings. Let T and U be two traces. Call $\mathcal{O}$ the set of total orders over $|T|$ that contain $\leqslant_T$ and for each $R \in \mathcal{O}$, call T_R the trace obtained from T by replacing the order with R. Let $T' = \bigoplus_{R\in\mathcal{O}} T_R$.

By proposition 9, $\langle T \mid U\rangle$ is the number of matchings between T and U. This means that if there are n matchings, then $\langle T \mid U\rangle = 1 + \cdots + 1$ with n occurrences of 1. By hypothesis $1 + 1 = 1$, so $\langle T \mid U\rangle$ is 1 if there is at least one matching and 0 otherwise. By the same argument, for all $R \in \mathcal{O}$ we have $\langle T_R \mid U\rangle \in \{0, 1\}$, hence $\langle T' \mid U\rangle$ is 1 if there is at least one R such that $\langle T_R \mid U\rangle = 1$ and 0 otherwise.

Assume $\langle T \mid U\rangle = 1$, and let σ be a matching between T and U. Then σ induces an order $\leqslant$ on $|T|$ such that $a \leqslant_T b$ and $\sigma(a) \leqslant_U \sigma(b)$ both imply $a \leqslant b$. Any completion R of $\leqslant$ into a total order yields a total ordering T_R of T such that $\langle T_R \mid U\rangle = 1$, which proves that $\langle T' \mid U\rangle = 1$.

Reciprocally, assume that $\langle T' \mid U\rangle = 1$, then there is an $R \in \mathcal{O}$ such that $\langle T_R \mid U\rangle = 1$, then there is a matching σ between T_R and U. Since the only difference between T_R and T is the order and $\leqslant_T$ is included in R, σ is also a matching between T and U, hence $\langle T \mid U\rangle = 1$. □

References

[1] Emmanuel Beffara. An algebraic process calculus. In *Proceedings of the twenty-third annual IEEE symposium on logic in computer science (LICS)*, pages 130–141, 2008.

[2] Michele Boreale and Fabio Gadducci. Processes as formal power series: a coinductive approach to denotational semantics. *Theoretical Computer Science*, 360:440–458, 2006.

[3] Michele Boreale and Davide Sangiorgi. A fully abstract semantics for causality in the π-calculus. *Acta Informatica*, 35(5):353–400, 1998.

[4] Gérard Boudol and Ilaria Castellani. A non-interleaving semantics for CCS based on proved transitions. *Fundamenta Informaticae*, XI:433–453, 1988.

[5] Silvia Crafa, Daniele Varacca, and Nobuko Yoshida. Compositional event structure semantics for the π-calculus. In *Proceedings of the 18th international conference on concurrency theory (CONCUR)*, volume 4703 of *Lecture Notes in Computer Science*, pages 317–332. Springer, 2007.

[6] Pierpaolo Degano and Corrado Priami. Proved trees. In *Proceedings of the 19th International Colloquium on Automata, Languages and Programming (ICALP)*, volume 623 of *Lecture Notes in Computer Science*, pages 629–640. Springer, 1992.

[7] Pierpaolo Degano and Corrado Priami. Non-interleaving semantics for mobile processes. *Theoretical Computer Science*, 216:237–270, 1999.

[8] Thomas Ehrhard and Olivier Laurent. Interpreting a finitary π-calculus in differential interaction nets. In Luís Caires and Vasco T. Vasconcelos, editors, *18th International Conference on Concurrency Theory (Concur)*, volume 4703 of *LNCS*, pages 333–348. Springer, September 2007.

[9] Thomas Ehrhard and Laurent Regnier. Differential interaction nets. In *Workshop on Logic, Language, Information and Computation*, 2004. Invited paper.

[10] Paul-André Melliès. Asynchronous games 2: the true concurrency of innocence. In *Proceedings of the 15th international conference on concurrency theory (CONCUR)*, volume 3170 of *Lecture Notes in Computer Science*, pages 448–465. Springer, 2004.

[11] Paul-André Melliès and Samuel Mimram. From asynchronous games to concurrent games. Submitted, September 2008.

[12] Ernst-Rüdiger Olderog and C. Anthony R. Hoare. Specification-oriented semantics for communicating processes. *Acta Informatica*, 23(1):9–66, 1986.

[13] Davide Sangiorgi. Locality and interleaving semantics in calculi for mobile processes. *Theoretical Computer Science*, 155, 1996.

[14] Glynn Winskel. Event structure semantics for CCS and related languages. In *Proceedings of the 9th international colloquium on automata, languages and programming (ICALP)*, volume 140 of *Lecture Notes in Computer Science*, pages 561–576. Springer, July 1982.

A Technical proofs

A.1 Homotopy (proposition 1)

The basic case is $p = ab$ and $q = ba$ for some a and b with $a \mathrel{/\!\!/} b$. We thus prove that for any pair of transitions $P \xrightarrow{a} Q \xrightarrow{b} R$ with $a \mathrel{/\!\!/} b$, there is a term Q' such that $P \xrightarrow{b} Q' \xrightarrow{a} R$. Proceed by induction on the derivation of $P \xrightarrow{a} Q$.

- The case of the action rule $\alpha.P \xrightarrow{\alpha:\varepsilon} \_P$ cannot happen since no position is independent of ε but b is supposed to be independent of $\alpha : \varepsilon$.
- In the case of the $\_$ rule, we have $\_P \xrightarrow{1.a} \_Q \xrightarrow{1.b} \_R$ and we can proceed by induction on $P \xrightarrow{a} Q \xrightarrow{b} R$.
- In the case of the interaction rule, we have $a = (1.\iota, 2.\kappa)$ for some positions ι and κ, and the second transition starts from $(\boldsymbol{\nu}x)(P' \mid Q'[x/y])$. Reason by case analysis on the shape of this second transition. If all positions in b start with 1, then $b = 1.b'$ for some b' and the second transition comes from $P' \xrightarrow{b'} P''$, so we can apply the induction hypothesis on $P \xrightarrow{u^{\varepsilon}(x):1.\iota} P' \xrightarrow{b'} P''$ to get transitions $P \xrightarrow{b'} R \xrightarrow{u^{\varepsilon}(x):1.\iota} P''$, from which we deduce $P|Q \xrightarrow{b} R|Q \xrightarrow{a} (\boldsymbol{\nu}x)(P''|Q')$. If all positions in b start with 2, the same argument applies, the substitution of x for y is innocuous since it only affects actions prefixed by $u^{\neg\varepsilon}(y)$. If $b = (1.\iota', 2.\kappa')$ for some ι' and κ', then we have $P' \xrightarrow{v^{\eta}(x')\iota'} P''$ and $Q' \xrightarrow{v^{\neg\eta}(y')\kappa'} Q''$, so we can apply the induction hypothesis on P and Q independently, from which we deduce $P \mid Q \xrightarrow{b} (\boldsymbol{\nu}x')(P''' \mid Q'''[x'/y']) \xrightarrow{a} (\boldsymbol{\nu}x')(\boldsymbol{\nu}x)(P'' \mid Q''[x'/y', x/y])$, which concludes this case since the substitutions $[x/y]$ and $[x'/y']$ are independent and the order of restrictions is irrelevant.
- The $(\boldsymbol{\nu}x)$ context rule is obvious.
- In the right context rule for parallel composition, we have $a = 1.a'$ for some a'. If $b = 2.b'$ for some b', then a occurs in P and b occurs in Q, so they obviously commute. If b has the form $\alpha : 1.\iota$, then we proceed by induction in P. If b is a label (ι, κ) with one of ι, κ starting with 1, then we proceed by induction on the visible action at this position, in a similar way as for parallel composition.
- The other context rules for composition with and without interaction are similar.

The general case follows.

A.2 Testing equivalence is a congruence (theorem 1)

Consider a pair of equivalent processes $P \simeq Q$. Let α be an arbitrary action, we first prove that $\alpha.P \simeq \alpha.Q$. Let R be an arbitrary process. The set $\mathcal{R}(\alpha.P \mid R)$ can be split into two parts: the set $\mathcal{R}_0$ of runs where the action α is not triggered and the set $\mathcal{R}_1$ of runs in which it is. Then for each run $\rho \in \mathcal{R}_1$, there is a position ι such that $(1, 2.\iota) \in \rho$. Let ρ_1 be the partial run $\{ a \mid a \in \rho, a \leqslant_\rho (1, 2.\iota) \}$, that is the minimal run that triggers α; we have $(\alpha.P|R)/\rho_1 = (\boldsymbol{\nu}x)(P|R')$ for some R'; let $\rho_2 = \rho \setminus \rho_1$, so that ρ_2 is a run of $P \mid R'$ and $(\alpha.P \mid R)/\rho = (\boldsymbol{\nu}x)(P \mid R')/\rho_2$. Let $\mathcal{S}$ be the set of triples (ρ_1, R', ρ_2) for all $\rho \in \mathcal{R}_1$. Obviously $\mathcal{R}(\alpha.P \mid R)$ is in bijection with $\mathcal{R}_0 \uplus \mathcal{S}$ and

$$\langle \alpha.P \mid R \rangle = \sum_{2.\rho \in \mathcal{R}_0} s(R/\rho) + \sum_{(\rho_1, R', \rho_2) \in \mathcal{S}} s((P \mid R')/\rho_2)$$

Now let $\mathcal{L} = \{ (\rho_1, R') \mid \exists \rho_2, (\rho_1, R', \rho_2) \in \mathcal{S} \}$, and let $(\rho_1, R') \in \mathcal{L}$. Since $\mathcal{R}_1$ contains all runs of $\alpha.P \mid R$ that trigger α, it contains all the runs of $P \mid R'$ since $P \mid R'$ can be reached from $\alpha.P \mid R$, so we have $\{ \rho_2 \mid (\rho_1, R', \rho_2) \in \mathcal{S} \} = \mathcal{R}(P \mid R')$, hence

$$\sum_{(\rho_1,R',\rho_2)\in\mathcal{S}} s((P \mid R')/\rho_2) = \sum_{(\rho_1,R')\in\mathcal{L}} \sum_{\rho_2\in\mathcal{R}(P|R')} s((P \mid R')/\rho) = \sum_{(\rho_1,R')\in\mathcal{L}} \langle P \mid R' \rangle$$

By hypothesis, for all R' we have $\langle P \mid R' \rangle = \langle Q \mid R' \rangle$ so

$$\langle \alpha.P \mid R \rangle = \sum_{r\rho\in\mathcal{R}_0} s(R/\rho) + \sum_{(\rho_1,R')\in\mathcal{L}} \langle Q \mid R' \rangle = \langle \alpha.Q \mid R \rangle$$

since the reasoning above equally applies to Q. Therefore we get $\alpha.P \simeq \alpha.Q$.

For parallel composition, let R and S be arbitrary terms, we want to prove $\langle (P \mid R) \mid S \rangle = \langle (Q \mid R) \mid S \rangle$, in order to get $P \mid R \simeq Q \mid R$. Let φ be the function over positions such that for all ι, $\varphi(1.1.\iota) = 1.\iota$, $\varphi(1.2.\iota) = 2.1.\iota$ and $\varphi(2.\iota) = 2.\iota$, and for all path p, let $\varphi(p)$ be the path obtained by applying φ on all positions in p. Then φ is a bijection between the paths of $(P \mid R) \mid S$ and those of $P \mid (R \mid S)$, and it preserves homotopy so it actually provides a bijection between $\mathcal{R}((P \mid R) \mid S)$ and $\mathcal{R}(P \mid (R \mid S))$. Moreover, for all $\rho \in \mathcal{R}((P \mid R) \mid S)$, we have $s(((P \mid R) \mid S)/\rho) = s((P \mid (R \mid S))/\varphi(\rho))$, so $\langle (P \mid R) \mid S \rangle = \langle P \mid (R \mid S) \rangle$. Similarly we get $s((Q \mid R) \mid S) = \langle Q \mid (R \mid S) \rangle$, and by hypothesis we have $P \simeq Q$ so $\langle P \mid (R \mid S) \rangle = \langle Q \mid (R \mid S) \rangle$, from which we conclude.

For parallel composition without interaction, let R and S be arbitrary terms, we want to prove $\langle (P \parallel R) \mid S \rangle = \langle (Q \parallel R) \mid S \rangle$, in order to get $P \parallel R \simeq Q \parallel R$. The technique used for parallel composition with interaction does not apply here, because there is no simple form of associativity between the two parallel compositions. However, if the free names of P and R are disjoint, it is easily seen that $P \mid R$ and $P \parallel R$ are equivalent, and this is the fact we will use here.

Let A be a set of pairs (ι, κ) where ι is the position of an action in R and κ is the position of an action in S, such that these actions are on a free name and may interact with each other, and such that A is a partial injection (each position of R occurs at most once on the left, each position of S occurs at most once on the right). Call this kind of set a synchronization and let $\mathcal{S}$ be the set of all synchronizations. We say that a run $\rho \in \mathcal{R}((P \parallel R) \mid S)$ satisfies A, written $\rho \Vdash A$, if the interactions between R and S in ρ are exactly those designated by A, that is if $\{ (\iota, \kappa) \mid (1.2.\iota, 2.\kappa) \in \rho \} = A$.

We will define R^A and S^A to be rewritings of R and S such that the pairs (ι, κ) are guaranteed to interact. For this purpose, for each $(\iota, \kappa) \in A$, let $a_{\iota,\kappa}$ and $w_{\iota,\kappa}$ be fresh names: $a_{\iota,\kappa}$ is a new name on which the pair will interact (in order to avoid conflicts with other names) and $w_{\iota,\kappa}$ will act as a witness of (ι, κ), that will ensure that the pair actually interacts. Define R^A as the term R in which each action $a^\varepsilon(x).T$ at a position ι such that there is an $(\iota, \kappa) \in A$ is replaced by $a^\varepsilon_{\iota,\kappa}(x).(T \mid w_{\iota,\kappa}.1)$, and define S^A as the term S in which each action $a^\varepsilon(x).T$ at a position κ such that there is an $(\iota, \kappa) \in A$ is replaced by $a^\varepsilon_{\iota,\kappa}(x).T$ (without $w_{\iota,\kappa}$). Let W_A be any parallel composition of $w_{\iota,\kappa}.0 \mid \bar{w}_{\iota,\kappa}.1$ for all $\iota, \kappa \in A$.

If we now examine the runs of $(P \mid R^A) \mid (S^A \mid W_A)$, we observe that if a run ρ does not trigger the actions of a given pair $(\iota, \kappa) \in A$, then it must contain the reduction of $w_{1,j}.0 \mid \bar{w}_{\iota,\kappa}.1$ into $\_0 \mid \_1$ (because runs are made of maximal paths), so the outcome of this run is 0. On the other hand, if all the interactions given by A occur in ρ, it is still possible that some of the $w_{\iota,\kappa}.0 \mid \bar{w}_{\iota,\kappa}.1$ reduce into $\_0 \mid \_1$, but there is one possibility that each $\bar{w}_{\iota,\kappa}.1$ interacts with the $w_{\iota,\kappa}.1$ in R^A. From a run that satisfies this condition, we can deduce a unique run of $(P \parallel R) \mid S$ that satisfies A, and reciprocally from a run of $(P \parallel R) \mid S$ that satisfies A we can deduce a unique run of $(P \mid R^A) \mid (S^A \mid W_A)$ that does not reduce any $w_{\iota,\kappa}.0$. Moreover, this bijection between runs preserves outcomes, so $\langle (P \mid R^A) \mid (S^A \mid W_A) \rangle$ is the sum of all $s(((P \parallel R) \mid S)/\rho)$ for all runs ρ that satisfy A. From this we get the following decomposition:

$$\begin{aligned}\langle (P \parallel R) \mid S\rangle &= \sum_{A\in\mathcal{S}} \sum_{\rho \Vdash A} s(((P \parallel R) \mid S)/\rho) = \sum_{A\in\mathcal{S}} \big\langle (P \mid R^A) \mid (S^A \mid W_A)\big\rangle \\ &= \sum_{A\in\mathcal{S}} \big\langle P \mid (R^A \mid (S^A \mid W_A))\big\rangle = \sum_{A\in\mathcal{S}} \big\langle Q \mid (R^A \mid (S^A \mid W_A))\big\rangle = \langle (Q \parallel R) \mid S\rangle\end{aligned}$$

The equality $\big\langle (P \mid R^A) \mid (S^A \mid W_A)\big\rangle = \big\langle P \mid (R^A \mid (S^A \mid W_A))\big\rangle$ is justified by the same argument as above for parallel composition, and the substitution of Q for P is the hypothesis $P \simeq Q$. The final equality is the same reasoning for Q as for P above.

The equality $\langle (\boldsymbol{\nu} x)P \mid R\rangle = \langle (\boldsymbol{\nu} x)Q \mid R\rangle$ is justified by the fact that $\langle (\boldsymbol{\nu} x)P \mid R\rangle$ and $\langle P \mid R\rangle$ are equal if the name x is fresh with respect to R.

A.3 Basic equivalences (proposition 3)

For commutativity of composition with interaction, consider three terms P, Q, R. We first establish a bijection between $\mathcal{R}((P \mid Q) \mid R)$ and $\mathcal{R}((Q \mid P) \mid R)$. Let φ be the function over positions that exchanges *ll* and 1.2 at the beginning of words, i.e. $\varphi(1.1.\iota) = 1.2.\iota$, $\varphi(1.2.\iota) = 1.1.\iota$ and $\varphi(2.\iota) = 2.\iota$ for all position ι. For all path p, define $\varphi(p)$ as the path obtained by applying φ to all positions in p. Then clearly, for all path p of $(P|Q)|R$, $\varphi(p)$ is a path of $(Q|P)|R$. Moreover, for all paths p and q, $p \approx q$ if and only if $\varphi(p) \approx \varphi(q)$. Therefore φ is a bijection between $\mathcal{R}((P|Q)|R)$ and $\mathcal{R}((Q|P)|R)$. Besides, since $\mathbb{K}$ is commutative, we have $m((P|Q)|R/p) = m((Q|P)|R/\varphi(p))$ for all P, Q, R and p, so we have $\langle (P \mid Q) \mid R\rangle = \langle (Q \mid P) \mid R\rangle$.

For associativity, we use the same technique with relabeling function defined as $\varphi(1.1.1.\iota) = 1.1.\iota$, $\varphi(1.1.2.\iota) = 1.2.1.\iota$, $\varphi(1.2.\iota) = 1.2.2.\iota$ for all ι and $\varphi(\kappa) = \kappa$ for all other positions κ; the final argument is associativity of the product in $\mathbb{K}$. For neutrality, we use $\varphi(1.1.\iota) = \varphi(1.\iota)$ for all ι and $\varphi(\kappa) = \kappa$ for all other positions κ, and conclude by the neutrality of 1 in $\mathbb{K}$.

For parallel composition without interaction, the exact same arguments apply. For the non-interaction rule, a similar argument applies, using the fact that there can never be any interaction between Q and R if they do not share any free name (this property is specific of the πI calculus).

For the scoping rules, we simply remark that $\langle (\boldsymbol{\nu} x)P \mid Q\rangle = \langle P \mid Q\rangle$ if x is a fresh name, since names have no influence on outcomes.

For the place-holder rule, $\langle \_P \mid Q\rangle = \langle P \mid Q\rangle$ is proved by applying the function φ such that $\varphi(1.1.\iota) = 1.\iota$ for all ι and $\varphi(\kappa)$ for all other κ. This establishes a bijection between $\mathcal{R}(\_P \mid Q)$ and $\mathcal{R}(P \mid Q)$ since the $\_$ is never involved in any transition.

For the inaction rule, remark that in a term $(\boldsymbol{\nu} u)u^\varepsilon(x).P \mid R$, there can be no transition involving $u^\varepsilon(x)$, hence all runs are made of labels of the form $(2.\iota, 2.\kappa)$, so the runs of $(\boldsymbol{\nu} u)u^\varepsilon(x).P|$ R are the runs of R with an extra 2 in front of each position, moreover the outcomes are the same since $s((\boldsymbol{\nu} u)u^\varepsilon(x).P) = 1$.

For the non-interference rule, remark that all runs of $(\boldsymbol{\nu} u)(u(x).P \mid \bar{u}(x).Q) \mid R$ contain the transition $(1.1, 1.2)$, because of maximality and the fact that R cannot provide actions on u. The reduct by this transition is $(\boldsymbol{\nu} ux)(\_P \,|\, \_Q) \,|\, R$, and its runs are those of the original term without $(1.1, 1.2)$, so it has the same outcome. We thus have $(\boldsymbol{\nu} u)(u(x).P \mid \bar{u}(x).Q) \simeq (\boldsymbol{\nu} ux)(\_P \mid \_Q)$, and the equivalence $(\boldsymbol{\nu} ux)(\_P \mid \_Q) \simeq (\boldsymbol{\nu} ux)(P \mid Q)$ follows from the previous rules.

A.4 The module of processes (proposition 4)

We first show that, for all terms P, Q and R, $\langle (P \oplus Q) \mid R\rangle = \langle P \mid R\rangle + \langle Q \mid R\rangle$. Consider $\mathcal{R}((P \oplus Q) \mid R) = \mathcal{R}((\boldsymbol{\nu} u)((u.P \mid u.Q) \mid \bar{u}.1) \mid R)$. It is clear that any run contains an interaction of $\bar{u}.1$ with either $u.P$ or $u.Q$, since none of these may interact with anything else. We can thus write $\mathcal{R}((P \oplus Q) \mid R) = \mathcal{R}_1 \uplus \mathcal{R}_2$ where $\mathcal{R}_1$ is the set of runs that contain $(1.1.1, 1.2)$ and $\mathcal{R}_2$ is the set of runs that contain $(1.1.2, 1.2)$. The runs in $\mathcal{R}_1$ are the runs of $(\boldsymbol{\nu} u)((u.P \,|\, 1) \,|\, \bar{u}) \,|\, R$ and each of these runs has the same outcome in both terms, so

$$\sum_{\rho \in \mathcal{R}_1} s\big(((P \oplus Q) \mid R)/\rho\big) = \langle (\boldsymbol{\nu} u)((u.P \mid 1) \mid \bar{u}) \mid R \rangle = \langle P \mid R \rangle$$

by the equivalences of table 2. By a similar argument, we get the same for $\mathcal{R}_2$ and $\langle Q \mid R \rangle$ so we finally get $\langle (P \oplus Q) \mid R \rangle = \langle P \mid R \rangle + \langle Q \mid R \rangle$.

This equality and the fact that $(\mathbb{K}, +, 0)$ is a commutative monoid immediately implies that $(\Pi_{\mathbb{K}}, \oplus, 0)$ is a commutative monoid (where 0 is the atomic term with outcome 0).

For any terms P and Q and any outcome k, it is clear that $\langle (k \mid P) \mid Q \rangle = k \, \langle P \mid Q \rangle$, since the term k has no transition and contributes k multiplicatively to all outcomes of the term. This directly implies that the operation $k \cdot P$ has all required properties.

For the bilinearity of compositions, consider arbitrary terms P, Q, R, S. By previous results, we have

$$\begin{aligned} \langle (P \mid (Q \oplus R)) \mid S \rangle &= \langle (Q \oplus R) \mid (P \mid S) \rangle = \langle Q \mid (P \mid S) \rangle + \langle R \mid (P \mid S) \rangle \\ &= \langle (P \mid Q) \mid S \rangle + \langle (P \mid R) \mid S \rangle = \langle ((P \mid Q) \oplus (P \mid R)) \mid S \rangle \end{aligned}$$

This proves that parallel composition distributes over $\oplus$, and the fact that 0 is absorbing is equivalent to the rule $0 \cdot P \simeq 0$. The same rules for parallel composition without interaction can be proved by similar arguments about the partition of $\mathcal{R}(P \parallel (Q \oplus R))$ into runs that choose Q and runs that choose R.

For hiding, consider arbitrary terms P, Q, R and let x be a name. Assume (without loss of generality) that x does not occur in R. Then we have

$$\begin{aligned} \langle (\boldsymbol{\nu} x)(P \oplus Q) \mid S \rangle &= \langle (P \oplus Q) \mid S \rangle \\ &= \langle P \mid S \rangle + \langle Q \mid S \rangle = \langle (\boldsymbol{\nu} x)P \mid S \rangle + \langle (\boldsymbol{\nu} x)Q \mid S \rangle = \langle ((\boldsymbol{\nu} x)P \oplus (\boldsymbol{\nu} x)Q) \mid S \rangle \end{aligned}$$

The equivalence $(\boldsymbol{\nu} x)0 \simeq 0$ is one of the rules of table 2.

A.5 Linear actions and inactions (proposition 5)

We first prove $\alpha.P \simeq \hat{\alpha}.P \oplus \alpha.0$. Consider an arbitrary term Q call $\mathcal{R}_1$ the set of runs of $\alpha.P \,|\, Q$ that contain a transition $(1, \iota)$, i.e. runs that trigger α, and let $\mathcal{R}_0$ be the set of runs that do not. The runs of $\mathcal{R}_0$ are also runs of $\alpha.0 \,|\, Q$, moreover for each run $\rho \in \mathcal{R}(\alpha.0 \,|\, Q) \setminus \mathcal{R}_0$ the action α is triggered so 0 contributes to the outcome and $s((\alpha.0 \,|\, Q)/\rho) = 0$, hence $\sum_{\rho \in \mathcal{R}_0} s((\alpha.P \,|\, Q)/\rho) = \langle \alpha.0 \,|\, Q \rangle$. Now consider a run $\rho \in \mathcal{R}_1$. By definition, there is a κ such that $(1, \kappa) \in \rho$. We deduce from ρ a run ρ' of $\hat{\alpha}.P$ as follows: let φ be the function that maps each $1.1.\iota$ to $1.1.1.1.\iota$ and all other positions to themselves; set $\rho' := \varphi(\rho \setminus (1, \kappa)) \cup \{(1.1, \kappa), (1.1.1.2, 1.2.2)\}$. This literally means that ρ' is ρ where all positions in P are shifted to reflect their positions in $(\boldsymbol{\nu} w)(\alpha.(P \mid w.1) \mid (w.0 \mid \bar{w}.0)) \mid Q$, $(1, \kappa)$ is shifted to reflect the new position of α, and the interaction between $w.1$ and $\bar{w}.1$ is added (which is valid since it is freed when α is triggered). Clearly ρ' is a run of $\hat{\alpha}.P \mid Q$ and $s((\hat{\alpha}.P \mid Q)/\rho') = s((\alpha.P \mid Q)/\rho)$. The mapping $\rho \mapsto \rho'$ is objective, and its image is the set of runs of $\hat{\alpha}.P \mid Q$ that trigger $w.1$. By maximality, any other run of $\hat{\alpha}.P \mid Q$ must trigger $w.0$, hence the outcome of all other runs is 0, which implies $\langle \hat{\alpha}.P \mid Q \rangle = \sum_{\rho \in \mathcal{R}_1} s((\alpha.P \,|\, Q)/\rho)$. We can finally deduce $\langle \alpha.P \,|\, Q \rangle = \langle \alpha.0 \,|\, Q \rangle + \langle \hat{\alpha}.P \,|\, Q \rangle$ and conclude.

For linearity, we use the fact that $\langle \hat{\alpha}.P \mid Q\rangle$ is the sum of the $s((\hat{\alpha}.P \mid Q)/\rho)$ for the runs ρ that actually trigger α (and the witness action $w.1$). If $P = k \mid P'$, these runs are the same in $\hat{\alpha}.(k \mid P') \mid Q$ and $\hat{\alpha}.(1 \mid P') \mid Q$, but the outcomes are multiplied by k in the first case, so $\langle \hat{\alpha}.(k \mid P') \mid Q\rangle = k \cdot \langle \hat{\alpha}.(1 \mid P') \mid Q\rangle$ and $\hat{\alpha}.(k \mid P') \simeq k \mid \hat{\alpha}.(1 \mid P') \simeq k \mid \hat{\alpha}.P'$. If $P = P_1 \oplus P_2$, the choice is eventually active in all relevant runs, so each of these runs triggers either P_1 or P_2. We can thus establish a bijection between $\mathcal{R}(\hat{\alpha}.(P_1 \oplus P_2) \mid Q)$ and the disjoint union of $\mathcal{R}(\hat{\alpha}.P_1 \mid Q)$ and $\mathcal{R}(\hat{\alpha}.P_2 \mid Q)$. Since outcomes are preserved by this bijection, we finally get $\langle \hat{\alpha}.(P_1 \oplus P_2) \mid Q\rangle = \langle \hat{\alpha}.P_1 \mid Q\rangle + \langle \hat{\alpha}.P_2 \mid Q\rangle$ and $(P_1 \oplus P_2) \mid Q \simeq (P_1 \mid Q) \oplus (P_2 \mid Q)$.

The equivalence $(\boldsymbol{\nu} u)u^\varepsilon(x).P \simeq 0$ can be deduced from previous equations:

$$\begin{aligned}
(\boldsymbol{\nu} u)u^\varepsilon(x).P &= (\boldsymbol{\nu} uw)(u^\varepsilon(x).(P \mid w.1) \mid (w.0 \mid \bar{w}.1)) \\
&\simeq (\boldsymbol{\nu} w)((\boldsymbol{\nu} u)u^\varepsilon(x).(P \mid w.1) \mid (w.0 \mid \bar{w}.1)) \\
&\simeq (\boldsymbol{\nu} w)(1 \mid (w.0 \mid \bar{w}.1)) \simeq (\boldsymbol{\nu} w)(w.0 \mid \bar{w}.1) \simeq (\boldsymbol{\nu} w)(0 \mid 1) \simeq 0
\end{aligned}$$

For the equivalence $\hat{\alpha}.(\beta.0 \mid P) \simeq \beta.0 \mid \hat{\alpha}.P$, assuming the subject of β is not the bound name of action α, let Q be an arbitrary term and consider $\mathcal{R}(\hat{\alpha}.(\beta.0 \mid P) \mid Q)$. Any run that does not trigger $\hat{\alpha}$ or that triggers both $\hat{\alpha}$ and β has outcome 0, so the only relevant runs are those that trigger $\hat{\alpha}$ but not β. Clearly these runs are in bijection with the runs of $(\beta.0 \mid \hat{\alpha}.P) \mid Q$ that trigger $\hat{\alpha}$ and not β, by a simple rewriting of the positions. Moreover, this bijection preserves outcomes, so the sums of the outcomes of these runs are the same. A similar argument proves $\hat{\alpha}.(\beta.0 \parallel P) \simeq \beta.0 \parallel \hat{\alpha}.P$.

For the composition of inactions, the relevant runs of a term $(\alpha.0 \mid \alpha.0) \mid P$ or $(\alpha.0 \parallel \alpha.0) \mid P$ are those that do not trigger any occurrence of α, so the number of such occurrences does not matter. Finally, we get $\alpha.O \mid \bar{\alpha}.0 \simeq 0$ by the remark that all runs of $(\alpha.0 \mid \bar{\alpha}.0) \mid P$ must trigger one of the inactions: either $\alpha.0$ interacts with P, or $\bar{\alpha}.0$ interacts with P, or none of these happen and $\alpha.0$ and $\bar{\alpha}.0$ must interact together, by maximality of runs.

A.6 Interpretation of partial terms (proposition ??)

First, remark that for all $P \sqsubseteq_f P'$, $\langle P' \mid 0\rangle = 0$, hence $\langle P \mid 0\rangle$ so $[\![P]\!]$ is defined on 0. Now assume $[\![P]\!]$ is defined on Q and R, for all $P \sqsubseteq_f P'$ we have $\langle P' \mid (Q \oplus R)\rangle = \langle P' \mid Q\rangle + \langle P' \mid R\rangle = [\![P]\!](Q) + [\![P]\!](R)$ so $[\![P]\!]$ is correctly defined on $Q \oplus R$. The same argument applies for $[\![P]\!](k \cdot Q) = k \cdot [\![P]\!](Q)$. As a consequence, $[\![P]\!]$ is indeed a partial behaviour.

Let P, Q, R be partial terms. The relation

$$\{ ((P' \mid Q') \mid R', (Q' \mid P') \mid R') \mid P \sqsubseteq_f P', Q \sqsubseteq_f Q', R \sqsubseteq_f R' \}$$

is obviously a bijection between total refinements of $(P \mid Q) \mid R$ and total refinements of $(Q \mid P) \mid R$, and this bijection preserves outcomes because of the equation $P \mid Q \simeq Q \mid P$ for total terms. As a consequence we have $\langle (P \mid Q) \mid R\rangle = \langle (Q \mid P) \mid R\rangle$ for all R, which implies $[\![P \mid Q]\!] = [\![Q \mid P]\!]$.

The same argument applies for all other equations. For scope extrusion and non-interaction, we use the fact that indeterminates have a fixed set of free names. For the equations in which a sub-term is duplicated (distribution of compositions over $\oplus$), we use the fact that all occurrences of a given indeterminate are replaced by the same term when refining.

If P is a partial term and Q is a refinement of P obtained by injectively renaming the indeterminates of P, then for all total R we clearly have $P \sqsubseteq R$ if and only if $Q \sqsubseteq R$, so $P \simeq Q$.

Let P, P', Q be partial terms such that $P \simeq P'$ and $\operatorname{ind}(P) \cap \operatorname{ind}(Q) = \operatorname{ind}(P') \cap \operatorname{ind}(Q) = \emptyset$. Then the refinements of $P \mid Q$ are the compositions of a refinement of P and a refinement of Q, chosen independently since $\operatorname{ind}(P) \cap \operatorname{ind}(Q) = \emptyset$. Let R be an arbitrary total term. If $\langle (P \mid Q) \mid R\rangle$ is defined and has value k, then for all refinements $P \sqsubseteq_f P''$ and $Q \sqsubseteq_f Q''$ we have $\langle (P'' \mid Q'') \mid R \rangle = k$ so $\langle (P \mid Q'') \mid R \rangle = k$, therefore $\langle (P' \mid Q'') \mid R \rangle$ is defined and has value k, hence $\langle (P' \mid Q) \mid R \rangle = k$ and $P' \mid Q \simeq P \mid Q$. Analogous reasoning yields $P' \parallel Q \simeq P \parallel Q$. Preservation of equivalence by other syntactic constructs is immediate.

A.7 Implementation of traces (proposition 7)

The fact that $\{T\}$ is simple is obvious by definition of $\{T\}$.

Let us first build an exhaustive pre-trace of $\{T\}$. Let $(a_i)_{1 \leqslant i \leqslant n}$ be a topological ordering of $|T|$. We deduce a sequence of terms $(P_i)_{1 \leqslant i \leqslant n+1}$ such that for each $i < n$ there is an interaction from P_i to P_{i+1} made of a transition $\mathrm{act}(a_i) : \iota$ and internal transitions. Let $P_1 = \{T\}$. Let i be an integer such that $1 \leqslant i \leqslant n$, assume P_i is a reduct of $\{T\}$ that contains the $\hat{\mathrm{act}}(a_j)$ for all $j \geqslant i$ and in active position all the $\hat{\hat{x}}_{a_j a_k}$ such that $j < i \leqslant k$ and $a_j < a_k$. Then the term $A^T_{a_i}$ occurs in active position in P_i and the prefix $\{\hat{x}_{a_j a_i}\}_{a_j < a_i}$ can be consumed, which puts $\hat{\mathrm{act}}(a_i)$ in active position. We can then apply a transition $\mathrm{act}(a_i) : \iota$ for some ι followed by an internal transition that consumes the $w.1$ contained in the linear action (as of definition 8). This puts in active position the $\hat{\hat{y}}_{a_{i+1} a_j}$ for all $a_j > a_i$, and each of these can interact with the $\hat{y}_{a_i a_j}.\hat{\hat{x}}_{a_i a_j}$, which puts in active position the $\hat{\hat{x}}_{a_i a_j}$. By this interaction we reach a state P_{i+1} that satisfies the condition we assumed on P_i. Applying this method until $i = n$ gives a term P_{n+1} in which everything except the $u^{\varepsilon}.0$ has been consumed, so this provides a exhaustive pre-trace ρ of $\{T\}$.

Now, let ρ' be another exhaustive pre-trace of $\{T\}$. By definition, ρ and ρ' trigger the same actions in $\{T\}$. From this we can deduce that ρ and ρ' contain the same transition labels, indeed the actions $\hat{\mathrm{act}}(a)$ are necessarily consumed by visible transitions since they are joined together by a composition without interaction and the only composition with interaction they are involved in is with the names x_{ab} and y_{ab}. On the other hand, all actions on these names are consumed by internal transitions, and for each such name there is exactly one linear input and one linear output so there is only one possible internal transition for each name. As a consequence the sets of actions of ρ and ρ' are the same so $\rho = \rho'$.

Let us now prove that $\rho^* = T$. The only thing we have to check is that the causal order of ρ is the order of T. First consider two events $a, b \in |T|$ with $a < b$. The action $\hat{\mathrm{act}}(b)$ in $\{T\}$ is prefixed by $\hat{x}_{ab}$ (and possibly other actions), and $\hat{\hat{x}}_{ab}$ is prefixed by $\hat{y}_{ab}$, which is itself prefixed by $\hat{\mathrm{act}}(a)$, so the transition $\mathrm{act}(a)$ is before the transition $\mathrm{act}(b)$ in ρ. Then consider two incomparable events a and b. There is a topological ordering of $|T|$ that places a before b and another that places b before a, so by the construction above we can construct an interaction in ρ for each case, which proves that the transitions $\mathrm{act}(a)$ and $\mathrm{act}(b)$ are incomparable in the causal order of ρ.

A.8 Decomposition into traces (proposition 8)

Let Q be a simple term. The term $P \mid Q$ is simple, so the outcome of a run of this term is either 1 or 0. Let ρ be a run with outcome 1. This implies that no inaction of $P \mid Q$ is triggered in ρ and that each linear action is triggered.

Call ρ^1 the projection of ρ on P. Formally, ρ^1 is obtained from ρ by replacing each transition $1.a$ with a, removing every transition $2.a$ and replacing each transition $(1.\iota, 2.\kappa)$ with the $\alpha : \iota$ that is the left premise of the derivation of $(1.\iota, 2.\kappa)$. Note that the order on ρ^1 need not be the restriction to ρ^1 of the order on ρ, it is only a subset of this order. Call ρ^2 the analogous projection on Q.

Since the outcome of ρ is 1, the pre-traces ρ^1 and ρ^2 are exhaustive pre-traces of P and Q respectively. Let ρ' be the unique exhaustive pre-trace of $\big\{(\rho^1)^*\big\}$. By construction, there is a bijection between the positions of the visible actions of ρ^1 and those of ρ', which establishes a bijection between runs of $P \mid Q$ with outcome 1 that project on P as ρ^1:

$$\left\{ \vartheta \mid \vartheta \in \mathcal{R}(P \mid Q),\ \vartheta^1 = \rho^1,\ s((P \mid Q)/\vartheta) = 1 \right\}$$

and runs of $\left\{(\rho^1)^*\right\} \mid Q$ with outcome 1:

$$\left\{ \vartheta \mid \vartheta \in \mathcal{R}(\left\{(\rho^1)^*\right\} \mid Q),\ s((\left\{(\rho^1)^*\right\} \mid Q)/\vartheta) = 1 \right\}.$$

This bijection preserves outcomes, so we have

$$\sum_{\substack{\sigma \in \mathcal{R}_e(P|Q) \\ \sigma^1 = \rho^1}} s((P \mid Q)/\sigma) = \left\langle \left\{(\rho^1)^*\right\} \mid Q \right\rangle$$

Summing for all potential values of ρ^1, i.e. all exhaustive pre-traces of P, yields

$$\langle P \mid Q \rangle = \sum_{\rho^1 \in \mathcal{P}_e(P)} \sum_{\substack{\sigma \in \mathcal{R}_e(P|Q) \\ \sigma^1 = \rho^1}} s((P \mid Q)/\sigma) = \sum_{\rho^1 \in \mathcal{P}_e(P)} \left\langle \left\{(\rho^1)^*\right\} \mid Q \right\rangle$$

from which we can conclude.

A.9 Trace interaction (proposition 9)

Let $P = \{T\} \mid \{U\}$. By proposition 8 we have $P \simeq \bigoplus_{\rho \in \mathcal{P}_e(P)} \{\rho^*\}$ hence $\langle P \rangle = \sum_{\rho \in \mathcal{P}_e(P)} \langle \{\rho^*\} \rangle$. Clearly, for all trace V, $\langle V \rangle$ is 1 if $|V| = \emptyset$ and 0 otherwise, so $\langle P \rangle$ is the number pre-traces $\rho \in \mathcal{P}_e(P)$ such that $|\rho^*|$ is empty.

Consider such a pre-trace ρ, by definition ρ triggers all linear actions in $\{T\}$ and $\{U\}$, so ρ^1 and ρ^2 are the unique exhaustive pre-traces of $\{T\}$ and $\{U\}$ respectively. The relation $\{ (\iota, \kappa) \mid (1.\iota, 2.\kappa) \in \rho \}$ establishes a bijection between positions of actions in $\{T\}$ and $\{U\}$, which implies a bijection $\sigma : |T| \to |U|$. Clearly, for all $a \in |T|$, we have $p_U(\sigma(a)) = \neg p_T(a)$ since an action can only interact with an action of the opposite polarity. It is also easy to prove that $s_U(\sigma(a)) = \sigma(s_T(a))$, since two actions that interact are either on the same public name or on private names that are unified by the interaction of previous actions. Consider two transitions (ι_a, κ_a) and (ι_b, κ_b) in ρ, that correspond to the pairs of actions $(a, \sigma(a))$ and $(b, \sigma(b))$: if $a \leqslant_T b$ then the action at ι_a must occur before the action at ι_b, so $(\iota_a, \kappa_a) \leqslant (\iota_b, \kappa_b)$; the same argument applies if $\sigma(a) \leqslant_U \sigma(b)$, so the order $\leqslant_\rho$ contains the orders $\leqslant_T$ and $\leqslant_U$, which proves that the union of these orders is acyclic. Finally, if there were $\varepsilon \in \boldsymbol{P}$ and $x \in \boldsymbol{N} \uplus |T|$ such that $(\varepsilon, x) \in N_T$ and $(\neg\varepsilon, \sigma(x)) \in N_U$, then the run ρ could be extended with an interaction between the inactions associated with them, and the outcome would be 0. Therefore $\sigma \in \mathcal{S}(T, U)$.

Reciprocally, let σ be a synchronization of T and U. Since the relation $\{ (a, b) \mid a \leqslant_T b \text{ or } \sigma(a) \leqslant_U \sigma(b) \}$ is acyclic, there is a non-decreasing enumeration $|T| = \{a_1, \ldots, a_n\}$ such that $\sigma(a_1), \ldots, \sigma(a_n)$ is also non-decreasing. Then there is a path $p \in \{T\}$ that reaches $a_1, \ldots, a_n$ in this order and a run $q \in \{U\}$ that reaches $\sigma(a_1), \ldots, \sigma(a_n)$ in this order. By combining p and q we get a path $r \in P$. Indeed, for each i we have $p(\sigma(a_i)) = \neg p(a_i)$ and $s(\sigma(a_i)) = \sigma(s(a_i))$ so either a_i and $\sigma(a_i)$ have the same public name as subject, or their subjects are two bound names $z_{s(a_i)}$ and $z_{s(\sigma(a_i))}$. Since $s(a_i) < a_i$ by definition, there is $j < i$ such that $s(a_i) = a_j$ and then $s(\sigma(a_i)) = \sigma(a_j)$, so the subjects of a_i and $\sigma(a_i)$ are unified by the interaction between a_j and $\sigma(a_j)$. In any case, the actions a_i and $\sigma(a_i)$ can interact. The term P/r is the composition with interaction of $\{T\}/p$ and $\{U\}/q$, and these terms are compositions without interaction of the inactions that correspond to N_T and N_U respectively. The condition that $(\neg\varepsilon, \sigma(x)) \notin N_U$ for all $(\varepsilon, x) \in N_T$ guarantees that no further interaction can occur, therefore r is a maximal path of P and $s(P/r) = 1$.

These construction establish a bijection between $\mathcal{S}(T, U)$ and the runs of $\{T\}$ and $\{U\}$ with outcome 1, which proves the expected result.