



**HAL**  
open science

# Types for Parallel Complexity in the Pi-calculus

Patrick Baillot, Alexis Ghyselen

► **To cite this version:**

Patrick Baillot, Alexis Ghyselen. Types for Parallel Complexity in the Pi-calculus. 2019. hal-02302544

**HAL Id: hal-02302544**

**<https://hal.science/hal-02302544>**

Preprint submitted on 3 Oct 2019

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Types for Parallel Complexity in the Pi-calculus

Patrick Baillot<sup>1</sup> and Alexis Ghyselen<sup>1</sup>

<sup>1</sup>Univ Lyon, CNRS, ENS de Lyon, Universite Claude-Bernard Lyon 1, LIP , F-69342, Lyon Cedex 07, France

## 1 Introduction

**Context** Certifying time complexity bounds for a program is a challenging question as it deals with properties which are important for predicting quantitative behaviour of software but which are of course undecidable. In the setting of sequential functional programs this problem, as well as the related one of time complexity inference, have been addressed using type systems (see e.g. [7, 2, 1]). These settings provide rich type systems such that if a program can be assigned a type, then one can extract from the type derivation a complexity bound for its execution on any input. The type system itself thus provides a complexity certification procedure, and if a type inference algorithm is also provided one obtains a complexity inference procedure. It is then quite natural to wonder whether similar kinds of analysis could be carried out for languages that can express parallel computation and concurrent behaviours, such as process calculi and in particular the  $\pi$ -calculus. In such a setting however sequential time complexity is not sufficient, and one would be more naturally interested in handling notions of parallel complexity, such as the *span* and the *work* of the system. This is the problem we wish to tackle in the present work.

**Approach** We want to be able to choose for different examples of systems the cost model we are interested in, e.g. should we count the number of emissions of messages, receptions, comparisons etc.? For this reason it will be convenient to consider an instrumented language, with a *tick* construction that we will use to mark the operations we want to count.

A second requirement that we have is that we wish to derive complexity bounds which are parametric with respect to the size of inputs, for instance which depend on the length of a list. For that it will be useful to have a language of types that can carry information about sizes, and this is why we take inspiration from size types. So data-types will be annotated with an index (or parameter) which will provide some information on the size of values. Moreover, as we want to bound the execution time and as we are in a setting of communication through channels, a second ingredient that we will use is that the typing of a channel will carry information about *when* communication will be performed on this channel. In order to be able to reason differently on bounds for emission and reception it will be convenient for us to use the approach of input/output types for  $\pi$ -calculus.

**Contributions** In this paper we define two type systems for the  $\pi$ -calculus which provide upper bounds respectively on the span and on the work complexity of a term. For that we first define a small-step operational semantics on the  $\pi$ -calculus with *tick*, which allows to characterize the span. Intuitively it performs reduction with maximal parallelism. We then introduce a type system of size types with temporal information. Typing judgements assign a complexity  $K$  to the typed process. We prove a soundness result, stating that if a process  $P$  can be typed and assigned a complexity  $K$ , then  $K$  bounds its reduction time in the operational semantics, hence its span complexity. We also describe a second small-step operational semantics corresponding to the work, and a variant of the first type system which provides a bound on the work complexity.

**Related Work** To the author's knowledge, the first work to capture parallel complexity by means of type was given by Kobayashi [9]. In this work, only the parallel communication complexity is considered and the notion of time appears both in syntax and types. A type contains *usages*, that is intuitively

a detailed description of its behaviour. With this, there is no need for time linearity as in our work. Moreover, the use of dependent types to have an extension of the type system was also proposed but not detailed. Then, Das, Hoffmann and Pfenning proposed a type system with temporal session types [3, 4] to capture several notions of complexity. In this work, time and complexity are captured in the type system by the use of temporal logic time modalities. However, the use of session-types imposes a strict linearity that we believe restricts the expressiveness of their programs.

The methodology of our work is inspired by implicit computational complexity, which aims at characterizing complexity classes by means of dedicated programming languages or logics, for instance by providing sequential languages whose programs characterize exactly the class of FPTIME functions. Some results have already been adapted to the concurrent case, but mainly for the work complexity and not for the span, e.g. [12] for a lambda-calculus with multithreading, [6] for a language of session types, [5] for  $\pi$ -calculus and [11] for a higher-order  $\pi$ -calculus. Contrarily to those works we do not restrict to a particular complexity class (like FPTIME) and we handle the case of the span.

Technically, the types we use are inspired from linear dependent types, introduced by Dal Lago and Gaboardi [2]. Those are one of the many variants and descendants of size types, which were first introduced by Hughes, Pareto and Sabry [8].

## 2 Pi-calculus with input/output types

We present here a classical  $\pi$ -calculus with input/output types. More detail about those types or  $\pi$ -calculus can be found in [13]. The set of *variables*, *expressions* and *pre-processes* are defined by the following grammar.

$$\begin{aligned}
v &:= x, y, z \mid a, b, c \\
e &:= v \mid 0 \mid \mathbf{s}(e) \mid [] \mid e :: e' \mid \mathbf{tt} \mid \mathbf{ff} \\
P, Q &:= 0 \mid P \mid Q \mid !a(\tilde{v}).P \mid a(\tilde{v}).P \mid \bar{a}(\tilde{e}) \mid (\nu a)P \mid \mathbf{match} \ e \ \mathbf{with} \ \{0 \mapsto P \mid \mathbf{s}(x) \mapsto Q\} \\
&\mid \mathbf{match} \ e \ \mathbf{with} \ \{\[] \mapsto P \mid x :: y \mapsto Q\} \mid \mathbf{if} \ e \ \mathbf{then} \ P \ \mathbf{else} \ Q
\end{aligned}$$

Variables  $x, y, z$  denote *base type variables*, so they represent integers, lists or booleans. Variables  $a, b, c$  denote *channel variables*. The notation  $\tilde{v}$  stands for a sequence of variables  $v_1, v_2, \dots, v_k$ . In the same way,  $\tilde{e}$  is a sequence of expressions. We work up to  $\alpha$ -renaming, and we use  $P[\tilde{v} := \tilde{e}]$  to denote the substitution of the free variables  $\tilde{v}$  in  $P$  by  $\tilde{e}$ .

We define on those pre-processes a congruence relation  $\equiv$ , such that this relation is the least congruence relation closed under:

$$\begin{aligned}
P \mid 0 &\equiv P & P \mid Q &\equiv Q \mid P & P \mid (Q \mid R) &\equiv (P \mid Q) \mid R & (\nu a)(\nu b)P &\equiv (\nu b)(\nu a)P \\
(\nu a)(P \mid Q) &\equiv (\nu a)P \mid Q & & & & & & \text{(when } a \text{ is not free in } Q)
\end{aligned}$$

Note that the last rule can always be made by renaming. Also, note that contrary to other congruence relation for the  $\pi$ -calculus, we do not consider the rule for replicated input ( $!P \equiv !P \mid P$ ), and  $\alpha$ -conversion is not an explicit rule in the congruence. With this definition, we can give a canonical form for pre-processes, as in [10].

**Definition 1** (Guarded Pre-processes and Canonical Form). *A pre-process is guarded if it is an input, a replicated input, an output or a conditional. We say that a pre-process is in canonical form if it has the form*

$$(\nu \tilde{a})(P_1 \mid \dots \mid P_n)$$

with  $P_1, \dots, P_n$  that are guarded pre-processes.

And we now show that all processes have a somewhat unique canonical form.

**Lemma 1** (Existence of Canonical Form). *For any pre-process  $P$ , there is a  $Q$  in canonical form such that  $P \equiv Q$ .*

|   |  |   |
|---|--|---|
| $\overline{!a(\tilde{v}).P \mid \bar{a}(\tilde{e}) \rightarrow !a(\tilde{v}).P \mid P[\tilde{v} := \tilde{e}]}$ | $\overline{a(\tilde{v}).P \mid \bar{a}(\tilde{e}) \rightarrow P[\tilde{v} := \tilde{e}]}$                            |   |
| $\overline{\text{match } 0 \text{ with } \{0 \mapsto P \mid s(x) \mapsto Q\} \rightarrow P}$                    | $\overline{\text{match } s(e) \text{ with } \{0 \mapsto P \mid s(x) \mapsto Q\} \rightarrow Q[x := e]}$              |   |
| $\overline{\text{match } [] \text{ with } \{[] \mapsto P \mid x :: y \mapsto Q\} \rightarrow P}$                | $\overline{\text{match } e :: e' \text{ with } \{[] \mapsto P \mid x :: y \mapsto Q\} \rightarrow Q[x, y := e, e']}$ |   |
| $\overline{\text{if } \text{tt} \text{ then } P \text{ else } Q \rightarrow P}$                                 | $\overline{\text{if } \text{ff} \text{ then } P \text{ else } Q \rightarrow Q}$                                      | $\frac{P \rightarrow Q}{P \mid R \rightarrow Q \mid R}$ |
| $\frac{P \rightarrow Q}{(\nu a)P \rightarrow (\nu a)Q}$   | $\frac{P \equiv P' \quad P' \rightarrow Q' \quad Q' \equiv Q}{P \rightarrow Q}$                                      |   |

Figure 1: Reduction Rules

*Proof.* Let us suppose that, by renaming, all the introduction of new variables have different names and that they also differ from the free variables already in  $P$ . We can then proceed by induction on the structure of  $P$ . The only interesting case is for parallel composition. Suppose that

$$P \equiv (\nu \tilde{a})(P_1 \mid \dots \mid P_n) \quad Q \equiv (\nu \tilde{b})(Q_1 \mid \dots \mid Q_m)$$

With  $P_1, \dots, P_n, Q_1, \dots, Q_m$  guarded pre-processes. Then, by hypothesis on the name of variables, we have  $\tilde{a}$  and  $\tilde{b}$  disjoint and  $\tilde{a}$  is not free in  $Q$ , as well as  $\tilde{b}$  is not free in  $P$ . So, we obtain

$$P \mid Q \equiv (\nu \tilde{a})(\nu \tilde{b})(P_1 \mid \dots \mid P_n \mid Q_1 \mid \dots \mid Q_m)$$

□

**Lemma 2** (Uniqueness of Canonical Form). *If*

$$(\nu \tilde{a})(P_1 \mid \dots \mid P_n) \equiv (\nu \tilde{b})(Q_1 \mid \dots \mid Q_m)$$

*with  $P_1, \dots, P_n, Q_1, \dots, Q_m$  guarded pre-processes, then  $m = n$  and  $\tilde{a}$  is a permutation of  $\tilde{b}$ . Moreover, for some permutation  $Q'_1, \dots, Q'_n$  of  $Q_1, \dots, Q_n$ , we have  $P_i \equiv Q'_i$  for all  $i$ .*

*Proof.* Recall that  $\alpha$ -renaming is not a rule of  $\equiv$ , otherwise this propriety would be false. As before, we suppose that all names are already well-chosen. Then, let us define a set **name** of channel variable and a multiset **gp** of guarded pre-processes.

- $\text{name}(0) = \emptyset$  and  $\text{gp}(0) = \emptyset$ .
- $\text{name}(P \mid Q) = \text{name}(P) \amalg \text{name}(Q)$  and  $\text{gp}(P \mid Q) = \text{gp}(P) + \text{gp}(Q)$ .
- $\text{name}(P) = \emptyset$  and  $\text{gp}(P) = [P]$ , when  $P$  is guarded.
- $\text{name}((\nu a)P) = \text{name}(P) \amalg \{a\}$  and  $\text{gp}((\nu a)P) = \text{gp}(P)$ .

Then, we can easily show the following lemma by definition of the congruence relation.

**Lemma 3.** *If  $P \equiv Q$  then  $\text{name}(P) = \text{name}(Q)$  and if  $\text{gp}(P) = [P_1, \dots, P_n]$  and  $\text{gp}(Q) = [Q_1, \dots, Q_m]$ , then  $m = n$  and for some permutation  $Q'_1, \dots, Q'_n$  of  $Q_1, \dots, Q_n$ , we have  $P_i \equiv Q'_i$  for all  $i$ .*

Finally, Lemma 2 is a direct consequence of Lemma 3. □

We can now define the reduction relation  $P \rightarrow Q$  for pre-processes. It is defined by the rules given in Figure 1. Remark that substitution should be well-defined in order to do the reduction. For example,  $(a(\tilde{v}).P)[a := \text{tt}]$  is not a valid substitution, as a channel variable is replaced by a boolean. More formally, channel variables must be substituted by other channel variables and base type variables can be substituted by any expression except channel variables. However, when we have typed pre-processes, this yields well-typed substitutions.

The set of *base types* and types are given by the following grammar.

|   |   |   |   |
|---|---|---|---|
| $\overline{\mathcal{B} \sqsubseteq \mathcal{B}}$  | $\frac{\tilde{T} \sqsubseteq \tilde{U} \quad \tilde{U} \sqsubseteq \tilde{T}}{\text{ch}(\tilde{T}) \sqsubseteq \text{ch}(\tilde{U})}$ | $\overline{\text{ch}(\tilde{T}) \sqsubseteq \text{in}(\tilde{T})}$    | $\overline{\text{ch}(\tilde{T}) \sqsubseteq \text{out}(\tilde{T})}$ |
| $\frac{\tilde{T} \sqsubseteq \tilde{U}}{\text{in}(\tilde{T}) \sqsubseteq \text{in}(\tilde{U})}$ | $\frac{\tilde{U} \sqsubseteq \tilde{T}}{\text{out}(\tilde{T}) \sqsubseteq \text{out}(\tilde{U})}$                                     | $\frac{T \sqsubseteq T' \quad T' \sqsubseteq T''}{T \sqsubseteq T''}$ |   |

Figure 2: Subtyping Rules

|  |  |   |  |
|--|--|---|--|
| $\frac{v : T \in \Gamma}{\Gamma \vdash v : T}$   | $\overline{\Gamma \vdash 0 : \text{Nat}}$            | $\frac{\Gamma \vdash e : \text{Nat}}{\Gamma \vdash \mathbf{s}(e) : \text{Nat}}$ | $\overline{\Gamma \vdash [] : \text{List}(\mathcal{B})}$ |
| $\frac{\Gamma \vdash e : \mathcal{B} \quad \Gamma \vdash e' : \text{List}(\mathcal{B})}{\Gamma \vdash e :: e' : \text{List}(\mathcal{B})}$ | $\overline{\Gamma \vdash \mathbf{tt} : \text{Bool}}$ | $\overline{\Gamma \vdash \mathbf{ff} : \text{Bool}}$                            |  |
| $\frac{\Delta \vdash e : U \quad \Gamma \sqsubseteq \Delta \quad U \sqsubseteq T}{\Gamma \vdash e : T}$                                    |  |   |  |

Figure 3: Typing Rules for Expressions

$$\mathcal{B} := \text{Nat} \mid \text{List}(\mathcal{B}) \mid \text{Bool} \quad T := \mathcal{B} \mid \text{ch}(\tilde{T}) \mid \text{in}(\tilde{T}) \mid \text{out}(\tilde{T})$$

When a type  $T$  is not a base type, we call it a *channel type*. Then, we define a subtyping relation on those types, expressed by the rules of Figure 2

**Definition 2** (Typing Contexts). *A typing context  $\Gamma$  is a sequence of hypotheses of the form  $x : \mathcal{B}$  or  $a : T$  where  $T$  is a channel type.*

We can now define typing for expressions and pre-processes. This is expressed by the rules of Figure 3 and Figure 4.

Finally, we can now show the following lemma.

**Lemma 4** (Closed Typed Normal Forms). *A pre-process  $P$  such that  $\vdash P$  is in normal form for  $\rightarrow$  if and only if*

$$P \equiv (\nu(a_1, \dots, a_n))(!b_1(\tilde{v}_1^0).P_1 \mid \dots \mid !b_k(\tilde{v}_k^0).P_k \mid c_1(\tilde{v}_1^1).Q_1 \mid \dots \mid c_{k'}(\tilde{v}_{k'}^1).Q_{k'} \mid \overline{d_1}\langle \tilde{e}_1 \rangle \mid \dots \mid \overline{d_{k''}}\langle \tilde{e}_{k''} \rangle)$$

with  $(\{b_i \mid 1 \leq i \leq k\} \cup \{c_i \mid 1 \leq i \leq k'\}) \cap \{d_i \mid 1 \leq i \leq k\} = \emptyset$ .

*Proof.* In order to show that, we first give an exhaustive list of possibilities for a reduction, as in [10].

**Lemma 5.** *If  $R \rightarrow R'$  then one of the following statements is true (where  $R_1, \dots, R_n$  are guarded pre-processes)*

- $$R \equiv (\nu \tilde{b})(R_1 \mid \dots \mid R_n \mid !a(\tilde{v}).P \mid \overline{a}\langle \tilde{e} \rangle) \quad R' \equiv (\nu \tilde{b})(R_1 \mid \dots \mid R_n \mid !a(\tilde{v}).P \mid P[\tilde{v} := \tilde{e}])$$

|   |   |  |  |
|---|---|--|--|
| $\overline{\Gamma \vdash 0}$  | $\frac{\Gamma \vdash P \quad \Gamma \vdash Q}{\Gamma \vdash P \mid Q}$  | $\frac{\Gamma \vdash a : \text{in}(\tilde{T}) \quad \Gamma, \tilde{v} : \tilde{T} \vdash P}{\Gamma \vdash !a(\tilde{v}).P}$  |  |
| $\frac{\Gamma \vdash a : \text{in}(\tilde{T}) \quad \Gamma, \tilde{v} : \tilde{T} \vdash P}{\Gamma \vdash a(\tilde{v}).P}$  | $\frac{\Gamma \vdash a : \text{out}(\tilde{T}) \quad \Gamma \vdash \tilde{e} : \tilde{T}}{\Gamma \vdash \overline{a}\langle \tilde{e} \rangle}$ | $\frac{\Gamma, a : T \vdash P}{\Gamma \vdash (\nu a)P}$  |  |
| $\frac{\Gamma \vdash e : \text{Nat} \quad \Gamma \vdash P \quad \Gamma, x : \text{Nat} \vdash Q}{\Gamma \vdash \text{match } e \text{ with } \{0 \mapsto P \mid \mathbf{s}(x) \mapsto Q\}}$ |   | $\frac{\Gamma \vdash e : \text{List}(\mathcal{B}) \quad \Gamma \vdash P \quad \Gamma, x : \mathcal{B}, y : \text{List}(\mathcal{B}) \vdash Q}{\Gamma \vdash \text{match } e \text{ with } \{[] \mapsto P \mid x :: y \mapsto Q\}}$ |  |
| $\frac{\Gamma \vdash e : \text{Bool} \quad \Gamma \vdash P \quad \Gamma \vdash Q}{\Gamma \vdash \text{if } e \text{ then } P \text{ else } Q}$  |   | $\frac{\Delta \vdash P \quad \Gamma \sqsubseteq \Delta}{\Gamma \vdash P}$  |  |

Figure 4: Typing Rules for Pre-Processes

- $R \equiv (\nu \tilde{b})(R_1 \mid \cdots \mid R_n \mid a(\tilde{v}).P \mid \overline{a}(\tilde{e})) \quad R' \equiv (\nu \tilde{b})(R_1 \mid \cdots \mid R_n \mid P[\tilde{v} := \tilde{e}])$
- $R \equiv (\nu \tilde{b})(R_1 \mid \cdots \mid R_n \mid \text{match } 0 \text{ with } \{0 \mapsto P \mid \mathbf{s}(x) \mapsto Q\}) \quad R' \equiv (\nu \tilde{b})(R_1 \mid \cdots \mid R_n \mid P)$
- $R \equiv (\nu \tilde{b})(R_1 \mid \cdots \mid R_n \mid \text{match } \mathbf{s}(e) \text{ with } \{0 \mapsto P \mid \mathbf{s}(x) \mapsto Q\}) \quad R' \equiv (\nu \tilde{b})(R_1 \mid \cdots \mid R_n \mid Q[x := e])$
- $R \equiv (\nu \tilde{b})(R_1 \mid \cdots \mid R_n \mid \text{match } [] \text{ with } \{[] \mapsto P \mid x :: y \mapsto Q\}) \quad R' \equiv (\nu \tilde{b})(R_1 \mid \cdots \mid R_n \mid P)$
- $R \equiv (\nu \tilde{b})(R_1 \mid \cdots \mid R_n \mid \text{match } e :: e' \text{ with } \{[] \mapsto P \mid x :: y \mapsto Q\}) \quad R' \equiv (\nu \tilde{b})(R_1 \mid \cdots \mid R_n \mid Q[x, y := e, e'])$
- $R \equiv (\nu \tilde{b})(R_1 \mid \cdots \mid R_n \mid \text{if } \mathbf{tt} \text{ then } P \text{ else } Q) \quad R' \equiv (\nu \tilde{b})(R_1 \mid \cdots \mid R_n \mid P)$
- $R \equiv (\nu \tilde{b})(R_1 \mid \cdots \mid R_n \mid \text{if } \mathbf{ff} \text{ then } P \text{ else } Q) \quad R' \equiv (\nu \tilde{b})(R_1 \mid \cdots \mid R_n \mid Q)$

*Proof.* By induction on  $R \rightarrow R'$ . All base cases are straightforward. Then, in parallel composition, we use Lemma 1 to obtain the correct form. The contextual rule for  $\nu$  is straightforward, and finally, the reduction up to congruence is straightforward using the transitivity of  $\equiv$ .  $\square$

We can now show Lemma 4. Suppose that

$$P \equiv (\nu(a_1, \dots, a_n))(!b_1(\tilde{v}_1^0).P_1 \mid \cdots \mid !b_k(\tilde{v}_k^0).P_k \mid c_1(\tilde{v}_1^1).Q_1 \mid \cdots \mid c_{k'}(\tilde{v}_{k'}^1).Q_{k'} \mid \overline{d_1}(\tilde{e}_1) \mid \cdots \mid \overline{d_{k''}}(\tilde{e}_{k''}))$$

with  $(\{b_i \mid 1 \leq i \leq k\} \cup \{c_i \mid 1 \leq i \leq k'\}) \cap \{d_i \mid 1 \leq i \leq k\} = \emptyset$ . By Lemma 2, this canonical form for  $P$  is unique. As  $P$  cannot have any of the possible form described in Lemma 5,  $P$  cannot be reduced by  $\rightarrow$  thus  $P$  is indeed in normal form for  $\rightarrow$ .

Conversely, suppose that  $P$  is in normal form for  $\rightarrow$ , with  $\vdash P$ . Let us write the canonical form:

$$P \equiv (\nu \tilde{a})(P_1 \mid \cdots \mid P_n)$$

First, let us show that there is no conditional in  $P_1, \dots, P_n$ . Indeed, if  $P_i$  has the form **if**  $e$  **then**  $R$  **else**  $R'$ , then by typing, we have  $\tilde{a} : \tilde{T} \vdash \text{if } e \text{ then } R \text{ else } R'$ . Thus, we obtain  $\tilde{a} : \tilde{T} \vdash e : \mathbf{Bool}$ . By definition of expressions, as all type in  $\tilde{T}$  must be channel types, we have  $e = \mathbf{tt}$  or  $e = \mathbf{ff}$ , thus  $P$  would not be in normal form for  $\rightarrow$ . Then, the canonical form can be written:

$$(\nu(a_1, \dots, a_n))(!b_1(\tilde{v}_1^0).P_1 \mid \cdots \mid !b_k(\tilde{v}_k^0).P_k \mid c_1(\tilde{v}_1^1).Q_1 \mid \cdots \mid c_{k'}(\tilde{v}_{k'}^1).Q_{k'} \mid \overline{d_1}(\tilde{e}_1) \mid \cdots \mid \overline{d_{k''}}(\tilde{e}_{k''}))$$

Now suppose, that  $a \in ((\{b_i \mid 1 \leq i \leq k\} \cup \{c_i \mid 1 \leq i \leq k'\}) \cap \{d_i \mid 1 \leq i \leq k\})$ . In the type derivation  $\vdash P$ ,  $a$  is given a channel type  $T$ . As a consequence, in the (replicated) input and in the output, the type of  $\tilde{v}$  in the input and  $\tilde{e}$  in the output corresponds, thus the substitution is well-defined and so  $P$  is reducible. This is absurd, thus  $(\{b_i \mid 1 \leq i \leq k\} \cup \{c_i \mid 1 \leq i \leq k'\}) \cap \{d_i \mid 1 \leq i \leq k\} = \emptyset$ , and we obtain the desired form.

This concludes the proof of Lemma 4.  $\square$

In the following, we will use a generalized version of Lemma 4, with exactly the same proof.

|  |  |  |  |  |
|--|--|--|--|--|
| $\overline{0 \Rightarrow 0}$   | $\overline{!a(\tilde{v}).P \Rightarrow !a(\tilde{v}).P}$ | $\overline{a(\tilde{v}).P \Rightarrow a(\tilde{v}).P}$                                       | $\overline{\bar{a}(\tilde{e}) \Rightarrow \bar{a}(\tilde{e})}$ | $\overline{\frac{P \Rightarrow P'}{(\nu a)P \Rightarrow (\nu a)P'}}$ |
| $\overline{\text{match } e \text{ with } \{0 \mapsto P \mid s(x) \mapsto Q\} \Rightarrow \text{match } e \text{ with } \{0 \mapsto P \mid s(x) \mapsto Q\}}$           |  |  |  |  |
| $\overline{\text{match } e \text{ with } \{\{\} \mapsto P \mid x :: y \mapsto Q\} \Rightarrow \text{match } e \text{ with } \{\{\} \mapsto P \mid x :: y \mapsto Q\}}$ |  |  |  |  |
| $\overline{\text{if } e \text{ then } P \text{ else } Q \Rightarrow \text{if } e \text{ then } P \text{ else } Q}$   |  |  |  |  |
| $\overline{\text{tick}.P \Rightarrow P}$   |  | $\overline{\frac{P \Rightarrow P' \quad Q \Rightarrow Q'}{P \mid Q \Rightarrow P' \mid Q'}}$ |  |  |

Figure 5: Time Reduction Rules

### 3 Size Types and Complexity

We enrich the previous set of pre-processes with a new constructor:  $\text{tick}.P$ . This new set of terms is called the set of *processes*. Intuitively,  $\text{tick}.P$  stands for "after one unit of time, the process continues as  $P$ ". We extend the congruence relation and typing to this new constructor, thus we add the following rule for congruence and for typing.

$$\frac{P \equiv Q}{\text{tick}.P \equiv \text{tick}.Q} \quad \frac{\Gamma \vdash P}{\Gamma \vdash \text{tick}.P}$$

A process of the form  $\text{tick}.P$  is considered a guarded process. Moreover,  $\text{tick}.P$  should be considered as a stuck process for the reduction  $\rightarrow$ . For example, the process  $a(\tilde{v}).P \mid \text{tick}.\bar{a}(\tilde{e})$  is not reducible for the relation  $\rightarrow$ . In order to reduce the tick, we define another reduction relation that stands for "one unit of time", thus, this new relation will be linked with our notion of complexity for our calculus.

#### 3.1 Time Reduction

The time reduction  $\Rightarrow$  is defined by the rules of Figure 5. Note that some processes have implicitly a "wait" instruction, for example a server or a process waiting for an input will always wait for its input according to this relation.

Note than for any process  $P$ , there is a unique  $Q$  such that  $P \Rightarrow Q$ . Note also that  $\Rightarrow$  allows the reduction of multiple ticks in parallel in one step. Indeed, we are here interested with the notion of *span* for the complexity, that is to say the complexity of a process under maximal parallelism. Let us first show that this relation  $\Rightarrow$  behaves well with the congruence relation.

**Lemma 6** (Time Reduction and Congruence). *If  $P \equiv Q$ ,  $P \Rightarrow P'$  and  $Q \Rightarrow Q'$  then  $P' \equiv Q'$ .*

*Proof.* By induction on  $P \equiv Q$ . All the base case are direct except the last one. For this one, we first need to show that if  $a$  is not free in  $Q$  and  $Q \Rightarrow Q'$  then  $a$  is not free in  $Q'$ , but this is an easy induction on the definition of  $\Rightarrow$ . Then, the case of reflexivity, symmetry and transitivity are straightforward, as well for contextual rules.  $\square$

As explained before, the relation  $\Rightarrow$  stands for one unit of time, and a reduction  $\rightarrow$  will be considered to take zero unit of time. Following this intuition, we impose a strategy of reduction for terms, saying that "before doing an expensive reduction ( $\Rightarrow$ ), we first reduce as much as possible using the zero-cost reduction ( $\rightarrow$ )". So the strategy we are interested in is the following one:

**Definition 3** (Reduction Strategy). *We define the tick-last strategy by the following steps:*

1. We start from a process  $P$ .
2. We reduce  $P$  to  $P'$  such that  $P \rightarrow^* P'$  and such that  $P'$  is in normal form for  $\rightarrow$ .
3.
  - If  $P' \Rightarrow P'$ , we stop the computation.
  - If  $P' \Rightarrow Q$  with  $Q \neq P'$ , then we go back to 1. with  $Q$  instead of  $P$

With this strategy comes a notion of complexity: the complexity of a reduction from  $P$  to  $Q$  with the tick-last strategy is the number of time reductions ( $\Rightarrow$ ) in the reduction. This corresponds to the *span* of a process, that is to say the complexity of a process with maximal parallelism. Indeed, in this strategy, a process first execute all zero-cost reduction, and then all guarded processes move forward one unit of time, that is to say all top guarded processes remove one tick or stay idle.

In the same way we showed previous lemmas for pre-processes, we obtain existence and uniqueness of the canonical form for processes, we can also give an exhaustive list for the shape of the reduction  $\rightarrow$  for processes as in Lemma 5 and we can deduce the following lemma.

**Lemma 7** (Typed Closed Normal Form with Tick). *A process  $P$  with  $\vdash P$  is in normal form for  $\rightarrow$  if and only if*

$$P \equiv (\nu(a_1, \dots, a_n))(!b_1(\tilde{v}_1^0).P_1 \mid \dots \mid !b_k(\tilde{v}_k^0).P_k \mid c_1(\tilde{v}_1^1).Q_1 \mid \dots \mid c_{k'}(\tilde{v}_{k'}^1).Q_{k'} \mid \bar{d}_1\langle \tilde{e}_1 \rangle \mid \dots \mid \bar{d}_{k''}\langle \tilde{e}_{k''} \rangle \mid \mathbf{tick}.R_1 \mid \dots \mid \mathbf{tick}.R_{k'''})$$

with  $(\{b_i \mid 1 \leq i \leq k\} \cup \{c_i \mid 1 \leq i \leq k'\}) \cap \{d_i \mid 1 \leq i \leq k\} = \emptyset$ .

Moreover, as for Lemma 5, we can express a generic form for the  $\Rightarrow$  relation.

**Lemma 8.** *If  $R \Rightarrow R'$ , then*

$$R \equiv (\nu\tilde{b})(R_1 \mid \dots \mid R_n \mid \mathbf{tick}.P_1 \mid \dots \mid \mathbf{tick}.P_n)$$

and

$$R' \equiv (\nu\tilde{b})(R_1 \mid \dots \mid R_n \mid P_1 \mid \dots \mid P_n)$$

where  $R_1, \dots, R_n$  are guarded processes that do not start with a tick.

From this lemma we can deduce that a process  $P$  satisfies  $P \Rightarrow P$  if and only if in the top guarded processes of its canonical form, none of them start with a tick.

Now, we show that the tick-last strategy is well-behaved according to the standard reduction in  $\pi$ -calculus. In order to do that, let us first introduce a notation for the erasure of ticks.

**Definition 4** (Eliminating Tick). *For a process  $P$ , we define a pre-process  $\lfloor P \rfloor$  corresponding to  $P$  in which all tick constructor have been erased.*

- $\lfloor 0 \rfloor = 0$
- $\lfloor P \mid Q \rfloor = \lfloor P \rfloor \mid \lfloor Q \rfloor$
- $\lfloor !a(\tilde{v}).P \rfloor = !a(\tilde{v}).\lfloor P \rfloor$
- $\lfloor a(\tilde{v}).P \rfloor = a(\tilde{v}).\lfloor P \rfloor$
- $\lfloor \bar{a}\langle \tilde{e} \rangle \rfloor = \bar{a}\langle \tilde{e} \rangle$
- $\lfloor (\nu a)P \rfloor = (\nu a)\lfloor P \rfloor$
- $\lfloor \mathbf{match} \ e \ \mathbf{with} \ \{0 \mapsto P \mid \mathbf{s}(x) \mapsto Q\} \rfloor = \mathbf{match} \ e \ \mathbf{with} \ \{0 \mapsto \lfloor P \rfloor \mid \mathbf{s}(x) \mapsto \lfloor Q \rfloor\}$
- $\lfloor \mathbf{match} \ e \ \mathbf{with} \ \{\square \mapsto P \mid x :: y \mapsto Q\} \rfloor = \mathbf{match} \ e \ \mathbf{with} \ \{\square \mapsto \lfloor P \rfloor \mid x :: y \mapsto \lfloor Q \rfloor\}$
- $\lfloor \mathbf{if} \ e \ \mathbf{then} \ P \ \mathbf{else} \ Q \rfloor = \mathbf{if} \ e \ \mathbf{then} \ \lfloor P \rfloor \ \mathbf{else} \ \lfloor Q \rfloor$
- $\lfloor \mathbf{tick}.P \rfloor = \lfloor P \rfloor$

And we can now show that the tick constructor and the tick-last strategy does not create new path of reduction in a term, and if the computation terminates, then we obtain a normal form for  $\rightarrow$ .

**Theorem 1.** *If a process  $P$  reduces to  $Q$  by the strategy of Definition 3, then  $Q$  is in normal form for  $\rightarrow$  and invariant by  $\Rightarrow$ . Moreover,  $\lfloor P \rfloor \rightarrow^* \lfloor Q \rfloor$  and  $\lfloor Q \rfloor$  is in normal form for  $\rightarrow$ .*

To begin with, remark that here the notation  $\rightarrow$  denote both the reduction relation on processes and the reduction relation on pre-processes. As those two relations are defined by the same rules, we keep the same notation for both.

*Proof.* The first part of this theorem is a direct consequence of Definition 3, as the computation stops only for processes invariant by  $\Rightarrow$ , and we only apply  $\Rightarrow$  to processes in normal form for  $\rightarrow$ .

In order to show the second part of this theorem, we must first prove the following lemmas.

**Lemma 9.** *If  $P \equiv Q$  then  $\lfloor P \rfloor \equiv \lfloor Q \rfloor$ .*

This can be shown directly by induction on  $\equiv$ .

**Lemma 10.** *If  $P \rightarrow Q$  then  $\lfloor P \rfloor \rightarrow \lfloor Q \rfloor$ .*

Again, this is straightforward by induction on  $\rightarrow$  using Lemma 9.

We can now prove Theorem 1 by recurrence on the number of time reduction ( $\Rightarrow$ ) from  $P$  to  $Q$ .

- If there are no time reduction from  $P$  to  $Q$ , then by definition of the strategy, we have  $P \rightarrow^* Q$ ,  $Q$  is in normal form for  $\rightarrow$  and  $Q \Rightarrow Q$ . By Lemma 10, we obtain  $\lfloor P \rfloor \rightarrow^* \lfloor Q \rfloor$ . Moreover, as  $Q \Rightarrow Q$ , by Lemma 8, the canonical form of  $Q$  has the shape  $(\nu \tilde{a})(Q_1 \mid \cdots \mid Q_n)$  where  $Q_1, \dots, Q_n$  are guarded processes that do not start with a tick. As a consequence, by Lemma 9,  $\lfloor Q \rfloor \equiv (\nu \tilde{a})(\lfloor Q_1 \rfloor \mid \cdots \mid \lfloor Q_n \rfloor)$ . As  $Q_1, \dots, Q_n$  do not start with a tick,  $\lfloor Q_i \rfloor$  has the same top constructor as  $Q_i$  for all  $i$ . Moreover,  $Q$  is in normal form for  $\rightarrow$ . Using Lemma 5, we can deduce that  $\lfloor Q \rfloor$  is also in normal form for  $\rightarrow$ . Indeed, if the canonical form of  $\lfloor Q \rfloor$  was one of those expressed in Lemma 5, then the canonical form of  $Q$  would have the same shape and so  $Q$  would not be in normal form for  $\rightarrow$ . This concludes this case.
- If there are at least one time reduction from  $P$  to  $Q$ , then by definition of the strategy, we have  $P \rightarrow^* P'$ ,  $P'$  in normal form for  $\rightarrow$  and  $P' \Rightarrow P''$  such that  $P''$  can be reduced to  $Q$  by the strategy. By Lemma 10, we have  $\lfloor P \rfloor \rightarrow^* \lfloor P' \rfloor$ . Moreover, with Lemma 8, we can see that if  $P' \Rightarrow P''$  then  $\lfloor P' \rfloor \equiv \lfloor P'' \rfloor$  by Lemma 9. Finally, by recurrence hypothesis, we have  $\lfloor P'' \rfloor \rightarrow^* \lfloor Q \rfloor$  and  $\lfloor Q \rfloor$  is in normal form for  $\rightarrow$ . Thus, we obtain  $\lfloor P \rfloor \rightarrow^* \lfloor Q \rfloor$  and  $\lfloor Q \rfloor$  is indeed in normal form for  $\rightarrow$ . This concludes this case.

Finally, we obtain Theorem 1. □

Remark that the tick-last strategy is not deterministic nor confluent, as  $\rightarrow$  is not. However, the tick constructor can enforce some reduction in a term. For example, following the strategy, the process  $a(\tilde{v}).P \mid \bar{a}(\tilde{e}) \mid \mathbf{tick}.\bar{a}(\tilde{e}')$  can only reduce to  $P[\tilde{v} := \tilde{e}] \mid \mathbf{tick}.\bar{a}(\tilde{e}')$  with  $\rightarrow$ , while without tick we have  $a(\tilde{v}).P \mid \bar{a}(\tilde{e}) \mid \bar{a}(\tilde{e}') \rightarrow \bar{a}(\tilde{e}) \mid P[\tilde{v} := \tilde{e}']$ . A consequence of this is that sometimes, adding a tick can enforce an infinite sequence of reduction by forbidding the terminating run. In a sense, the tick constructor allows the concept of race in a process. For example, the process  $a(\tilde{v}).\Omega \mid \bar{a}(\tilde{e}) \mid \mathbf{tick}.a(\tilde{v}).0$ , where  $\Omega$  is non terminating for  $\rightarrow$ , will always have infinite reductions.

Remark that with this concept of race, the tick-last strategy may not be the fastest way to reach a precise normal form. Take for example this process  $\mathbf{tick}!.a(\tilde{v}).P \mid !a(\tilde{v}).P' \mid \bar{a}(\tilde{e})$ . If  $P$  and  $P'$  has the same behaviour (for example sorting a list given on input and sending it to another channel) but  $P$  is faster than  $P'$ , then the tick-last strategy enforces to take the slower reduction.

### 3.2 Size Types with Temporal Information

We will now define a type system to bound the span of a process. The goal is to obtain a soundness result: if a process is typable then we can derive an integer  $K$  such that the complexity of any reduction following the strategy of Definition 3 is bounded by  $K$ .

Our type system relies on the definition of indices that give more information about the type. Those indices were for example used in [2] in the non-concurrent case. We also enrich type with temporal information, following the idea of [3] to obtain complexity bound.

**Definition 5.** *The set of indices for natural number is given by the following grammar.*

$$I, J, K := i, j, k \mid f(I_1, \dots, I_n)$$

*The variables  $i, j, k$  are called index variables. The set of index variables is denoted  $\mathcal{V}$ . We suppose given a set of function symbol containing for example the addition and the multiplication. We assume that each function symbol  $f$  comes with an interpretation  $\llbracket f \rrbracket : \mathbb{N}^{\text{ar}(f)} \rightarrow \mathbb{N}$ .*

Given an index valuation  $\rho : \mathcal{V} \rightarrow \mathbb{N}$ , we extend the interpretation of function symbols to indices, noted  $\llbracket I \rrbracket_\rho$  in the natural way. In an index  $I$ , the substitution of the occurrences of  $i$  in  $I$  by  $J$  is noted  $I\{J/i\}$ . We also assume that we have the subtraction as a function symbol, with  $n - m = 0$  when  $m \geq n$ .

**Definition 6** (Constraints on Indices). *Let  $\phi \subset \mathcal{V}$  be a set of index variables. A constraint  $C$  on  $\phi$  is an expression with the shape  $I \bowtie J$  where  $I$  and  $J$  are indices with free variables in  $\phi$  and  $\bowtie$  denotes a binary relation on integers. Usually, we take  $\bowtie \in \{\leq, <, =, \neq\}$ . Finite set of constraints are denoted  $\Phi$ .*

We say that a valuation  $\rho : \mathcal{V} \rightarrow \mathbb{N}$  satisfies a constraint  $I \bowtie J$ , noted  $\rho \models I \bowtie J$  when  $\llbracket I \rrbracket_\rho \bowtie \llbracket J \rrbracket_\rho$  holds. Similarly,  $\rho \models \Phi$  holds when  $\rho \models C$  for all  $C \in \Phi$ . Likewise, we note  $\phi; \Phi \models C$  when for all valuation  $\rho$  such that  $\rho \models \Phi$  we have  $\rho \models C$ .

**Definition 7.** *The set of types and base types are given by the following grammar.*

$$\begin{aligned} \mathcal{B} &:= \text{Nat}[I, J] \mid \text{List}[I, J](\mathcal{B}) \mid \text{Bool} \\ T &:= \mathcal{B} \mid \text{ch}_I(\tilde{T}) \mid \text{in}_I(\tilde{T}) \mid \text{out}_I(\tilde{T}) \mid \forall_I \tilde{i}. \text{serv}^K(\tilde{T}) \mid \forall_I \tilde{i}. \text{iserv}^K(\tilde{T}) \mid \forall_I \tilde{i}. \text{oserv}^K(\tilde{T}) \end{aligned}$$

A type  $\text{ch}_I(\tilde{T})$ ,  $\text{in}_I(\tilde{T})$  or  $\text{out}_I(\tilde{T})$  is called a *channel type* and a type  $\forall_I \tilde{i}. \text{serv}^K(\tilde{T})$ ,  $\forall_I \tilde{i}. \text{iserv}^K(\tilde{T})$  or  $\forall_I \tilde{i}. \text{oserv}^K(\tilde{T})$  is called a *server type*. For a channel type or a server type, the index  $I$  is called the *time* of this type, and for a server type, the index  $K$  is called the *complexity* of this type.

Intuitively, an integer  $n$  of type  $\text{Nat}[I, J]$  must be such that  $I \leq n \leq J$ . Likewise, a list of type  $\text{List}[I, J](\mathcal{B})$  have a size between  $I$  and  $J$ . To give a channel variable the type  $\text{ch}_I(\tilde{T})$  ensures that its communication should happen at time  $I$ . For example, a channel variable of type  $\text{ch}_0(\tilde{T})$  should do its communication before any tick occurs. Likewise, a name of type  $\forall_I \tilde{i}. \text{iserv}^K(\tilde{T})$  must be used in a replicated input, and this replicated input must be ready to receive for any time greater than  $I$ . Typically, a process  $\text{tick}.!a(\tilde{v}).P$  enforces that the type of  $a$  is  $\forall_I \tilde{i}. \text{iserv}^K(\tilde{T})$  with  $I$  greater than one, as the replicated input is not ready to receive at time 0.

Moreover, a server type has a kind of polymorphism for indices, and the index  $K$  stands for the complexity of the process spawned by this server. A typical example is a server taking as input a list and a channel, and send to this channel the sorted list, in time  $k \cdot n$  where  $n$  is the size of the list.

$$P = !a(x, b). \bar{b}(\text{sort}(x))$$

. Such a server name  $a$  could be given the type  $\forall_0 i. \text{serv}^{k \cdot i}(\text{List}[0, i](\mathcal{B}), \text{out}_{k \cdot i}(\text{List}[0, i](\mathcal{B})))$ . This means that this server is ready to receive an input and, for all integer  $i$ , if given a list of size at most  $i$  and an output channel doing its communication at time  $k \cdot i$  and waiting for a list of size at most  $i$ , the process spawned by this server will stop at time at most  $k \cdot i$ .

We define a notion of subtyping for size types. The rules are given in Figure 6.

The subtyping for channel type is standard, the only new thing is that we impose that the time of communication is invariant. Moreover, for servers, we can also change the complexity  $K$  in subtyping: for input servers, we can always define something faster than announced, and for output, we can always consider that a server is slower than announced.

In order to present to type system of our calculus, let us first introduce some notation.

**Definition 8** (Advancing Time in Types). *Given a set of index variables  $\phi$ , a set of constraint  $\Phi$ , a type  $T$  and an index  $I$ . We define  $T$  after  $I$  unit of time, denoted  $\langle T \rangle_{-I}^{\phi; \Phi}$  by:*

- $\langle \mathcal{B} \rangle_{-I}^{\phi; \Phi} = \mathcal{B}$
- $\langle \text{ch}_J(\tilde{T}) \rangle_{-I}^{\phi; \Phi} = \text{ch}_{(J-I)}(\tilde{T})$  if  $\phi; \Phi \models J \geq I$ . It is undefined otherwise. Other channel types follow exactly the same pattern.
- $\langle \forall_J \tilde{i}. \text{serv}^K(\tilde{T}) \rangle_{-I}^{\phi; \Phi} = \forall_{(J-I)} \tilde{i}. \text{serv}^K(\tilde{T})$  if  $\phi; \Phi \models J \geq I$ . Otherwise,  $\langle \forall_J \tilde{i}. \text{serv}^K(\tilde{T}) \rangle_{-I}^{\phi; \Phi} = \forall_{(J-I)} \tilde{i}. \text{oserv}^K(\tilde{T})$
- $\langle \forall_J \tilde{i}. \text{iserv}^K(\tilde{T}) \rangle_{-I}^{\phi; \Phi} = \forall_{(J-I)} \tilde{i}. \text{iserv}^K(\tilde{T})$  if  $\phi; \Phi \models J \geq I$ . It is undefined otherwise.

|  |   |  |
|--|---|--|
| $\frac{\phi; \Phi \models I' \leq I \quad \phi; \Phi \models J \leq J'}{\phi; \Phi \vdash \text{Nat}[I, J] \sqsubseteq \text{Nat}[I', J']}$  | $\frac{\phi; \Phi \models I' \leq I \quad \phi; \Phi \models J \leq J' \quad \phi; \Phi \vdash \mathcal{B} \sqsubseteq \mathcal{B}'}{\phi; \Phi \vdash \text{List}[I, J](\mathcal{B}) \sqsubseteq \text{List}[I', J'](\mathcal{B}')}$ |  |
| $\frac{}{\phi; \Phi \vdash \text{Bool} \sqsubseteq \text{Bool}}$   | $\frac{\phi; \Phi \models I = J \quad \phi; \Phi \vdash \tilde{T} \sqsubseteq \tilde{U} \quad \phi; \Phi \vdash \tilde{U} \sqsubseteq \tilde{T}}{\phi; \Phi \vdash \text{ch}_I(\tilde{T}) \sqsubseteq \text{ch}_I(\tilde{U})}$        | $\frac{}{\phi; \Phi \vdash \text{ch}_I(\tilde{T}) \sqsubseteq \text{in}_I(\tilde{T})}$   |
| $\frac{}{\phi; \Phi \vdash \text{ch}_I(\tilde{T}) \sqsubseteq \text{out}_I(\tilde{T})}$  | $\frac{\phi; \Phi \models I = J \quad \phi; \Phi \vdash \tilde{T} \sqsubseteq \tilde{U}}{\phi; \Phi \vdash \text{in}_I(\tilde{T}) \sqsubseteq \text{in}_I(\tilde{U})}$  | $\frac{\phi; \Phi \models I = J \quad \phi; \Phi \vdash \tilde{U} \sqsubseteq \tilde{T}}{\phi; \Phi \vdash \text{out}_I(\tilde{T}) \sqsubseteq \text{out}_I(\tilde{U})}$ |
| $\frac{\phi; \Phi \models I = J \quad (\phi, \tilde{i}); \Phi \vdash \tilde{T} \sqsubseteq \tilde{U} \quad (\phi, \tilde{i}); \Phi \vdash \tilde{U} \sqsubseteq \tilde{T} \quad (\phi, \tilde{i}); \Phi \models K = K'}{\phi; \Phi \vdash \forall_{I\tilde{i}}.\text{serv}^K(\tilde{T}) \sqsubseteq \forall_{J\tilde{i}}.\text{serv}^{K'}(\tilde{U})}$ |   |  |
| $\frac{}{\phi; \Phi \vdash \forall_{I\tilde{i}}.\text{serv}^K(\tilde{T}) \sqsubseteq \forall_{I\tilde{i}}.\text{iserv}^K(\tilde{T})} \quad \frac{}{\phi; \Phi \vdash \forall_{I\tilde{i}}.\text{serv}^K(\tilde{T}) \sqsubseteq \forall_{I\tilde{i}}.\text{oserv}^K(\tilde{T})}$  |   |  |
| $\frac{\phi; \Phi \models I = J \quad (\phi, \tilde{i}); \Phi \vdash \tilde{T} \sqsubseteq \tilde{U} \quad (\phi, \tilde{i}); \Phi \models K' \leq K}{\phi; \Phi \vdash \forall_{I\tilde{i}}.\text{iserv}^K(\tilde{T}) \sqsubseteq \forall_{J\tilde{i}}.\text{iserv}^{K'}(\tilde{U})}$   |   |  |
| $\frac{\phi; \Phi \models I = J \quad (\phi, \tilde{i}); \Phi \vdash \tilde{U} \sqsubseteq \tilde{T} \quad (\phi, \tilde{i}); \Phi \models K \leq K'}{\phi; \Phi \vdash \forall_{I\tilde{i}}.\text{oserv}^K(\tilde{T}) \sqsubseteq \forall_{J\tilde{i}}.\text{oserv}^{K'}(\tilde{U})}$   |   | $\frac{\phi; \Phi \vdash T \sqsubseteq T' \quad \phi; \Phi \vdash T' \sqsubseteq T''}{\phi; \Phi \vdash T \sqsubseteq T''}$  |

Figure 6: Subtyping Rules for Sized Types

- $\langle \forall_{J\tilde{i}}.\text{oserv}^K(\tilde{T}) \rangle_{-I}^{\phi; \Phi} = \forall_{(J-I)\tilde{i}}.\text{oserv}^K(\tilde{T})$ .

This definition can be extended to contexts, with  $\langle v : T, \Gamma \rangle_{-I}^{\phi; \Phi} = v : \langle T \rangle_{-I}^{\phi; \Phi}, \langle \Gamma \rangle_{-I}^{\phi; \Phi}$  if  $\langle T \rangle_{-I}^{\phi; \Phi}$  is defined. Otherwise,  $\langle v : T, \Gamma \rangle_{-I}^{\phi; \Phi} = \langle \Gamma \rangle_{-I}^{\phi; \Phi}$ . We will often omit the  $\phi; \Phi$  in the notation when it is clear from the context.

Let us precise a bit the definition here. Intuitively,  $T$  after  $I$  unit of time is the type  $T$  with a time decreased by  $I$ . For base types, there is no time thus nothing happens. Then, one can wonder what happens when the time of  $T$  is smaller than  $I$ . For non-server channel types, we consider that their time is over, thus we erase them from the context. For servers this is a bit more complicated. Intuitively, when a server is defined, it should stay available until the end. Thus, an output to a server should always be possible, no matter the time. However, there are also some time limitation in servers in the sense that we must respect the time limit to define a server. As a consequence, when time advances too much, we should not be able to define a server anymore. That is why servers lose their input capability when time advances too much. Let us now show that this definition behaves well with subtyping.

**Lemma 11.** *If  $\phi; \Phi \vdash T \sqsubseteq U$  then for any  $I$ , either  $\langle U \rangle_{-I}$  is undefined, or both  $\langle U \rangle_{-I}$  and  $\langle T \rangle_{-I}$  are defined, and  $\phi; \Phi \vdash \langle T \rangle_{-I} \sqsubseteq \langle U \rangle_{-I}$ .*

*Proof.* The proof is pretty straightforward by induction on  $\phi; \Phi \vdash T \sqsubseteq U$ . □

A corollary of Lemma 11 is that if  $\phi; \Phi \vdash \Gamma \sqsubseteq \Delta$ , then  $\langle \Gamma \rangle_{-I} = \Gamma', \Delta'$  with  $\phi; \Phi \vdash \Delta' \sqsubseteq \langle \Delta \rangle_{-I}$ .

**Definition 9.** *Given a set of index variables  $\phi$  and a set of constraints  $\Phi$ , a context  $\Gamma$  is said to be time invariant when it contains only base type variables or output server types  $\forall_{I\tilde{i}}.\text{oserv}^K(\tilde{T})$  with  $\phi; \Phi \models I = 0$ .*

Such a context is thus invariant by the operator  $\langle \cdot \rangle_{-I}$  for any  $I$ . This is typically the kind of context that we need to define a server. We can now present the type system. Rules are given in Figure 7 and Figure 8. A typing  $\phi; \Phi; \Gamma \vdash P \triangleleft K$  means intuitively that under the constraints  $\Phi$ , in the context  $\Gamma$ , a process  $P$  is typable and its complexity is bounded by  $K$ . And the typing for expressions  $\phi; \Phi; \Gamma \vdash e : T$  means that under the constraints  $\Phi$ , in the context  $\Gamma$ , the expression  $e$  can be given the type  $T$ .

The type system for expressions should not be very surprising. Still, remark that to type a channel name, the only possible rule is the subtyping one. In Figure 8, subtyping allows to increase the bound on the complexity. Then, the rule for parallel composition shows that we consider parallel complexity

|  |  |   |
|--|--|---|
| $\frac{v : T \in \Gamma}{\phi; \Phi; \Gamma \vdash v : T}$               | $\frac{}{\phi; \Phi; \Gamma \vdash 0 : \text{Nat}[0, 0]}$  | $\frac{\phi; \Phi; \Gamma \vdash e : \text{Nat}[I, J]}{\phi; \Phi; \Gamma \vdash \mathbf{s}(e) : \text{Nat}[I + 1, J + 1]}$   |
| $\frac{}{\phi; \Phi; \Gamma \vdash [] : \text{List}[0, 0](\mathcal{B})}$ | $\frac{\phi; \Phi; \Gamma \vdash e : \mathcal{B}}{\phi; \Phi; \Gamma \vdash e :: e' : \text{List}[I + 1, J + 1](\mathcal{B})}$ | $\frac{}{\phi; \Phi; \Gamma \vdash \mathbf{tt} : \text{Bool}}$  |
| $\frac{}{\phi; \Phi; \Gamma \vdash \mathbf{ff} : \text{Bool}}$           | $\frac{\phi; \Phi; \Delta \vdash e : U}{\phi; \Phi; \Gamma \vdash e : T}$  | $\frac{\phi; \Phi \vdash \Gamma \sqsubseteq \Delta \quad \phi; \Phi \vdash U \sqsubseteq T}{\phi; \Phi; \Gamma \vdash e : T}$ |

Figure 7: Typing Rules for Expressions

|   |   |
|---|---|
| $\frac{}{\phi; \Phi; \Gamma \vdash 0 \triangleleft 0}$  | $\frac{\phi; \Phi; \Gamma \vdash P \triangleleft K \quad \phi; \Phi; \Gamma \vdash Q \triangleleft K}{\phi; \Phi; \Gamma \vdash P \mid Q \triangleleft K}$  |
| $\frac{\phi; \Phi; \Gamma, \Delta \vdash a : \forall \tilde{i}. \text{iserv}^K(\tilde{T}) \quad (\phi, \tilde{i}); \Phi; \Gamma', \tilde{v} : \tilde{T} \vdash P \triangleleft K \quad \Gamma' \text{ time invariant} \quad \phi; \Phi \vdash \langle \Gamma \rangle_{-I}^{\phi; \Phi} \sqsubseteq \Gamma'}{\phi; \Phi; \Gamma, \Delta \vdash !a(\tilde{v}).P \triangleleft I}$     |   |
| $\frac{\phi; \Phi; \Gamma \vdash a : \text{in}_I(\tilde{T}) \quad \phi; \Phi; \langle \Gamma \rangle_{-I}, \tilde{v} : \tilde{T} \vdash P \triangleleft K}{\phi; \Phi; \Gamma \vdash a(\tilde{v}).P \triangleleft K + I}$   | $\frac{\phi; \Phi; \Gamma \vdash a : \text{out}_I(\tilde{T}) \quad \phi; \Phi; \langle \Gamma \rangle_{-I} \vdash \tilde{e} : \tilde{T}}{\phi; \Phi; \Gamma \vdash \bar{a}(\tilde{e}) \triangleleft I}$ |
| $\frac{\phi; \Phi; \Gamma \vdash a : \forall \tilde{i}. \text{oserv}^K(\tilde{T}) \quad \phi; \Phi; \langle \Gamma \rangle_{-I} \vdash \tilde{e} : \tilde{T}\{\tilde{J}/\tilde{i}\}}{\phi; \Phi; \Gamma \vdash \bar{a}(\tilde{e}) \triangleleft I + K\{\tilde{J}/\tilde{i}\}}$  | $\frac{\phi; \Phi; \Gamma, a : T \vdash P \triangleleft K}{\phi; \Phi; \Gamma \vdash (\nu a)P \triangleleft K}$   |
| $\frac{\phi; \Phi; \Gamma \vdash e : \text{Nat}[I, J] \quad \phi; (\Phi, I \leq 0); \Gamma \vdash P \triangleleft K \quad \phi; (\Phi, J \geq 1); \Gamma, x : \text{Nat}[I - 1, J - 1] \vdash Q \triangleleft K}{\phi; \Phi; \Gamma \vdash \text{match } e \text{ with } \{0 \mapsto P \mid \mathbf{s}(x) \mapsto Q\} \triangleleft K}$   |   |
| $\frac{\phi; \Phi; \Gamma \vdash e : \text{List}[I, J](\mathcal{B}) \quad \phi; (\Phi, I \leq 0); \Gamma \vdash P \triangleleft K \quad \phi; (\Phi, J \geq 1); \Gamma, x : \mathcal{B}, y : \text{List}[I - 1, J - 1](\mathcal{B}) \vdash Q \triangleleft K}{\phi; \Phi; \Gamma \vdash \text{match } e \text{ with } \{\square \mapsto P \mid x :: y \mapsto Q\} \triangleleft K}$ |   |
| $\frac{\phi; \Phi; \Gamma \vdash e : \text{Bool} \quad \phi; \Phi; \Gamma \vdash P \triangleleft K \quad \phi; \Phi; \Gamma \vdash Q \triangleleft K}{\phi; \Phi; \Gamma \vdash \text{if } e \text{ then } P \text{ else } Q \triangleleft K}$  | $\frac{\phi; \Phi; \langle \Gamma \rangle_{-1} \vdash P \triangleleft K}{\phi; \Phi; \Gamma \vdash \text{tick}.P \triangleleft K + 1}$  |
| $\frac{\phi; \Phi; \Delta \vdash P \triangleleft K \quad \phi; \Phi \vdash \Gamma \sqsubseteq \Delta \quad \phi; \Phi \models K \leq K'}{\phi; \Phi; \Gamma \vdash P \triangleleft K'}$   |   |

Figure 8: Typing Rules for Processes

as we take the maximum between the two processes instead of the sum. In the typing for input server, we integrate some weakening on context, and we want a time invariant process to type the server, as a server should not depend on the time. Note also that a server alone has no complexity, it is a call on this server that generates complexity, as we can see in the rule for output with server types. Some rules make the time advance in their continuation, for example the tick rule or input rule. This is expressed by the advance time operator on contexts.

Finally, remark that if we remove all size annotation and merge server types and channel types together to obtain back the types of Section 2, then all the rules of Figure 7 and Figure 8 are admissible in the type system of Figure 3 and Figure 4.

**Definition 10** (Forgetting Sizes). *Formally, given a sized type  $T$ , we define  $\mathcal{U}(T)$  the usual input/output type ( $\mathcal{U}$  is for forgetful) by:*

$$\begin{aligned} \mathcal{U}(\text{Nat}[I, J]) &:= \text{Nat} & \mathcal{U}(\text{List}[I, J](\mathcal{B})) &:= \text{List}(\mathcal{U}(\mathcal{B})) & \mathcal{U}(\text{Bool}) &:= \text{Bool} \\ \mathcal{U}(\text{ch}_I(\tilde{T})) &:= \text{ch}(\mathcal{U}(\tilde{T})) & \mathcal{U}(\text{in}_I(\tilde{T})) &:= \text{in}(\mathcal{U}(\tilde{T})) & \mathcal{U}(\text{out}_I(\tilde{T})) &:= \text{out}(\mathcal{U}(\tilde{T})) \\ \mathcal{U}(\forall \tilde{i}. \text{serv}^K(\tilde{T})) &:= \text{ch}(\mathcal{U}(\tilde{T})) & \mathcal{U}(\forall \tilde{i}. \text{iserv}^K(\tilde{T})) &:= \text{in}(\mathcal{U}(\tilde{T})) & \mathcal{U}(\forall \tilde{i}. \text{oserv}^K(\tilde{T})) &:= \text{out}(\mathcal{U}(\tilde{T})) \end{aligned}$$

Then, we obtain the following lemma.

**Lemma 12.** *If  $\phi : \Phi \vdash T \sqsubseteq T'$  then  $\mathcal{U}(T) \sqsubseteq \mathcal{U}(T')$ . Moreover, if  $\phi; \Phi; \Gamma \vdash e : T$  then  $\mathcal{U}(\Gamma) \vdash e : \mathcal{U}(T)$  and if  $\phi; \Phi; \Gamma \vdash P \triangleleft K$  then  $\mathcal{U}(\Gamma) \vdash P$*

*Proof.* Once we have weakening for input/output types and that advancing time does not change the underlying input/output type when it is defined, the proof can be made by induction on the subtyping derivation or the typing.  $\square$

## 4 Subject Reduction and Complexity Bound

In this section, we prove that our type system can indeed give a bound on the number of time reduction of a process following the strategy of Definition 3.

### 4.1 Intermediate Lemmas

We first show some usual and intermediate lemmas on the typing system.

**Lemma 13** (Weakening). *Let  $\phi, \phi'$  be disjoint set of index variables,  $\Phi$  be a set of constraint on  $\phi$ ,  $\Phi'$  be a set of constraints on  $(\phi, \phi')$ ,  $\Gamma$  and  $\Gamma'$  be contexts on disjoint set of variables.*

1. *If  $\phi; \Phi \vDash C$  then  $(\phi, \phi'); (\Phi, \Phi') \vDash C$ .*
2. *If  $\phi; \Phi \vdash T \sqsubseteq U$  then  $(\phi, \phi'); (\Phi, \Phi') \vdash T \sqsubseteq U$ .*
3. *If  $\phi; \Phi; \Gamma \vdash e : T$  then  $(\phi, \phi'); (\Phi, \Phi'); \Gamma, \Gamma' \vdash e : T$ .*
4.  *$\langle \Gamma \rangle_{-I}^{(\phi, \phi'); (\Phi, \Phi')} = \Delta, \Delta'$  with  $(\phi, \phi'); (\Phi, \Phi') \vdash \Delta \sqsubseteq \langle \Gamma \rangle_{-I}^{\phi; \Phi}$ .*
5. *If  $\phi; \Phi; \Gamma \vdash P \triangleleft K$  then  $(\phi, \phi'); (\Phi, \Phi'); \Gamma, \Gamma' \vdash P \triangleleft K$ .*

*Proof.* Point 1 is a direct consequence of the definition of  $\phi; \Phi \vDash C$ . Point 2 is proved by induction on the subtyping derivation, and it uses explicitly Point 1. Point 4 is a consequence of Point 1: everything that is defined in  $\langle \Gamma \rangle_{-I}^{\phi; \Phi}$  is also defined in  $\langle \Gamma \rangle_{-I}^{(\phi, \phi'); (\Phi, \Phi')}$ , and the subtyping condition is here since with more constraints, a server may not be changed into an output server by the advance of time. Point 3 and Point 5 are proved by induction on the typing derivation, and each point uses crucially the previous ones. Note that the weakening integrated in the rule for input servers is primordial to obtain Point 5. Note also that when the advance time operator is used, the weakened typing is obtained with the use of a subtyping rule.  $\square$

We also show that we can remove some useless hypothesis.

**Lemma 14** (Strengthening). *Let  $\phi$  be a set of index variables,  $\Phi$  be a set of constraint on  $\phi$ , and  $C$  a constraint on  $\phi$  such that  $\phi; \Phi \vDash C$ .*

1. *If  $\phi; (\Phi, C) \vDash C'$  then  $\phi; \Phi \vDash C'$ .*
2. *If  $\phi; (\Phi, C) \vdash T \sqsubseteq U$  then  $\phi; \Phi \vdash T \sqsubseteq U$ .*
3. *If  $\phi; (\Phi, C); \Gamma, \Gamma' \vdash e : T$  and the variables in  $\Gamma'$  are not free in  $e$ , then  $\phi; \Phi; \Gamma \vdash e : T$ .*
4.  $\langle \Gamma \rangle_{-I}^{\phi; (\Phi, C)} = \langle \Gamma \rangle_{-I}^{\phi; \Phi}$ .
5. *If  $\phi; (\Phi, C); \Gamma, \Gamma' \vdash P \triangleleft K$  and the variables in  $\Gamma'$  are not free in  $P$ , then  $\phi; \Phi; \Gamma \vdash P \triangleleft K$ .*

*Proof.* Point 1 is a direct consequence of the definition. Point 2 is proved by induction on the subtyping derivation. Point 4 is straightforward with Point 1 of this lemma and Point 1 of Lemma 13. Point 3 and Point 5 are proved by induction on the typing derivation.  $\square$

Then, we prove that index variables can indeed be substituted by any other indexes.

**Lemma 15** (Index Substitution). *Let  $\phi$  be a set of index variable and  $i \notin \phi$ . Let  $J$  be an index with free variables in  $\phi$ . Then,*

1.  $\llbracket I\{J/i\} \rrbracket_{\rho} = \llbracket I \rrbracket_{\rho[i \mapsto \llbracket J \rrbracket_{\rho}]}$ .
2. *If  $(\phi, i); \Phi \vDash C$  then  $\phi; \Phi\{J/i\} \vDash C\{J/i\}$ .*
3. *If  $(\phi, i); \Phi \vdash T \sqsubseteq U$  then  $\phi; \Phi\{J/i\} \vdash T\{J/i\} \sqsubseteq U\{J/i\}$ .*
4. *If  $(\phi, i); \Phi; \Gamma \vdash e : T$  then  $\phi; \Phi\{J/i\}; \Gamma\{J/i\} \vdash e : T\{J/i\}$ .*
5.  $\langle \Gamma\{J/i\} \rangle_{-I\{J/i\}}^{\phi; \Phi\{J/i\}} = \Delta, \Delta'$  with  $\phi; \Phi\{J/i\} \vdash \Delta \sqsubseteq (\langle \Gamma \rangle_{-I}^{(\phi, i); \Phi})\{J/i\}$ .
6. *If  $(\phi, i); \Phi; \Gamma \vdash P \triangleleft K$  then  $\phi; \Phi\{J/i\}; \Gamma\{J/i\} \vdash P \triangleleft K\{J/i\}$ .*

*Proof.* Point 1 is proved by induction on  $I$ . Then, Point 2 is a rather direct consequence of Point 1. Point 3 is proved by induction on the subtyping derivation, then Point 4 is proved by induction on the typing derivation. Point 5 is direct with the use of Point 2. And finally Point 6 is proved by induction on  $P$ . The induction is on  $P$  and not the typing derivation because of Point 5 that forces the use of weakening (Lemma 13).  $\square$

Those lemmas are rather usual in an index based system. However, the following one relies directly on our notion of time and the type system.

**Lemma 16** (Delaying). *Given a type  $T$  and an index  $I$ , we define the delaying of  $T$  by  $I$  units of time, denoted  $T_{+I}$ :*

$$\mathcal{B}_{+I} = \mathcal{B} \quad (\text{ch}_J(\tilde{T}))_{+I} = \text{ch}_{J+I}(\tilde{T})$$

*and for other channel and server types, the definition is the same as the one on the right above. This definition can be extended to contexts. With this, we have:*

1. *If  $\phi; \Phi \vdash T \sqsubseteq U$  then  $\phi; \Phi \vdash T_{+I} \sqsubseteq U_{+I}$ .*
2. *If  $\phi; \Phi; \Gamma \vdash e : T$  then  $\phi; \Phi; \Gamma_{+I} \vdash e : T_{+I}$ .*
3.  $\langle \Gamma_{+I} \rangle_{-J}^{\phi; \Phi} = \Delta, \Delta'$  with  $\phi; \Phi \vdash \Delta \sqsubseteq (\langle \Gamma \rangle_{-J}^{\phi; \Phi})_{+I}$ .
4.  $\langle \Gamma_{+I} \rangle_{-(J+I)} = \langle \Gamma \rangle_{-J}$ .
5. *If  $\phi; \Phi; \Gamma \vdash P \triangleleft K$  then  $\phi; \Phi; \Gamma_{+I} \vdash P \triangleleft K + I$ .*
6. *For any context  $\Gamma, \Gamma = \Gamma', \Delta$  with  $\phi; \Phi \vdash \Gamma' \sqsubseteq (\langle \Gamma \rangle_{-I})_{+I}$ .*

*Proof.* Point 1, Point 2, Point 3 and Point 4 are straightforward. Then, Point 5 is proved by induction on  $P$ . Point 4 is used on every rule for channel or servers, and Point 3 is used in the rule for tick. Point 6 is another straightforward proof. It is not used in the proof of Point 5 but it is useful for our subject reduction.  $\square$

We can now show the usual variable substitution lemmas.

**Lemma 17** (Substitution). *1. If  $\phi; \Phi; \Gamma, v : T \vdash e' : U$  and  $\phi; \Phi; \Gamma \vdash e : T$  then  $\phi; \Phi; \Gamma \vdash e'[v := e] : U$ .  
2. If  $\phi; \Phi; \Gamma, v : T \vdash P \triangleleft K$  and  $\phi; \Phi; \Gamma \vdash e : T$  then  $\phi; \Phi; \Gamma \vdash P[v := e] \triangleleft K$ .*

The proof is pretty straightforward.

We can now show the subject reduction of this calculus with the reduction  $\rightarrow$ .

## 4.2 Non-Quantitative Subject Reduction

The goal of this section is to prove the following theorem.

**Theorem 2** (Non-Quantitative Subject Reduction). *If  $\phi; \Phi; \Gamma \vdash P \triangleleft K$  and  $P \rightarrow Q$  then  $\phi; \Phi; \Gamma \vdash Q \triangleleft K$ .*

In order to do that, let us first show that the congruence relation behave well with typing.

**Lemma 18** (Congruence and Typing). *Let  $P$  and  $Q$  be processes such that  $P \equiv Q$ . Then,  $\phi; \Phi; \Gamma \vdash P \triangleleft K$  if and only if  $\phi; \Phi; \Gamma \vdash Q \triangleleft K$ .*

*Proof.* In fact, we will prove something more precise, by showing that the typing conserves the typing of channel name, so if we restrain our calculus with the constructor  $(\nu : T)$  to force the typing, the property still holds. Note that all previous lemmas also holds with this forced typing. We prove this by induction on  $P \equiv Q$ . Remark that for a process  $P$ , the typing system is not syntax-directed because of the subtyping rule. However, by reflexivity and transitivity of subtyping, we can always assume that a proof has exactly *one* subtyping rule before any syntax-directed rule. We first show this propriety for base case of congruence. The reflexivity is trivial then we have:

- **Case  $P \mid 0 \equiv P$ .** Suppose  $\phi; \Phi; \Gamma \vdash P \mid 0 \triangleleft K$ . Then the proof has the shape:

$$\frac{\frac{\frac{\pi}{\phi; \Phi; \Delta \vdash P \triangleleft K'}}{\phi; \Phi; \Delta \vdash P \mid 0 \triangleleft K'} \quad \frac{\frac{\phi; \Phi; \Delta' \vdash 0 \triangleleft 0 \quad \phi; \Phi \vdash \Delta \sqsubseteq \Delta'; 0 \leq K'}{\phi; \Phi; \Delta \vdash 0 \triangleleft K'}}{\phi; \Phi; \Delta \vdash P \mid 0 \triangleleft K'} \quad \phi; \Phi \vdash \Gamma \sqsubseteq \Delta; K' \leq K}{\phi; \Phi; \Gamma \vdash P \mid 0 \triangleleft K}$$

So, we can derive the following proof:

$$\frac{\frac{\pi}{\phi; \Phi; \Delta \vdash P \triangleleft K'} \quad \phi; \Phi \vdash \Gamma \sqsubseteq \Delta; K' \leq K}{\phi; \Phi; \Gamma \vdash P \triangleleft K}$$

Reciprocally, given a proof  $\pi$  of  $\phi; \Phi; \Gamma \vdash P \triangleleft K$ , we can derive the proof:

$$\frac{\frac{\pi}{\phi; \Phi; \Gamma \vdash P \triangleleft K} \quad \frac{\phi; \Phi; \Gamma \vdash 0 \triangleleft 0 \quad \phi; \Phi \vdash 0 \leq K}{\phi; \Phi; \Gamma \vdash 0 \triangleleft K}}{\phi; \Phi; \Gamma \vdash P \mid 0 \triangleleft K}$$

- **Case  $P \mid Q \equiv Q \mid P$ .** Suppose  $\phi; \Phi; \Gamma \vdash P \mid Q \triangleleft K$ . Then the proof has the shape:

$$\frac{\frac{\frac{\pi}{\phi; \Phi; \Delta \vdash P \triangleleft K'}}{\phi; \Phi; \Delta \vdash P \mid Q \triangleleft K'} \quad \frac{\frac{\pi'}{\phi; \Phi; \Delta \vdash Q \triangleleft K'}}{\phi; \Phi \vdash \Gamma \sqsubseteq \Delta; K' \leq K}}{\phi; \Phi; \Gamma \vdash P \mid Q \triangleleft K}$$

And so we can derive:

$$\frac{\frac{\pi'}{\phi; \Phi; \Delta \vdash Q \triangleleft K'} \quad \frac{\pi}{\phi; \Phi; \Delta \vdash P \triangleleft K'}}{\phi; \Phi; \Delta \vdash Q | P \triangleleft K'} \quad \frac{\phi; \Phi \vdash \Gamma \sqsubseteq \Delta; K' \leq K}{\phi; \Phi; \Gamma \vdash Q | P \triangleleft K}$$

We also have the reverse in the same way.

- **Case**  $P | (Q | R) \equiv (P | Q) | R$ . Suppose  $\phi; \Phi; \Gamma \vdash P | (Q | R) \triangleleft K$ . Then the proof has the shape:

$$\frac{\frac{\pi}{\phi; \Phi; \Delta \vdash P \triangleleft K'} \quad \frac{\frac{\pi'}{\phi; \Phi; \Delta' \vdash Q \triangleleft K''} \quad \frac{\pi''}{\phi; \Phi; \Delta' \vdash R \triangleleft K''}}{\phi; \Phi; \Delta' \vdash Q | R \triangleleft K''} \quad \frac{\phi; \Phi \vdash \Delta \sqsubseteq \Delta'; K'' \leq K'}{\phi; \Phi; \Delta \vdash Q | R \triangleleft K'}}{\phi; \Phi; \Delta \vdash P | (Q | R) \triangleleft K'} \quad \frac{\phi; \Phi \vdash \Gamma \sqsubseteq \Delta; K' \leq K}{\phi; \Phi; \Gamma \vdash P | (Q | R) \triangleleft K}$$

We can derive the proof:

$$\frac{\frac{\pi}{\phi; \Phi; \Delta \vdash P \triangleleft K'} \quad \frac{\frac{\pi'}{\phi; \Phi; \Delta' \vdash Q \triangleleft K''} \quad \frac{\phi; \Phi \vdash \Delta \sqsubseteq \Delta'; K'' \leq K'}{\phi; \Phi; \Delta \vdash Q \triangleleft K'}}{\phi; \Phi; \Delta \vdash P | Q \triangleleft K'} \quad \frac{\frac{\pi''}{\phi; \Phi; \Delta' \vdash R \triangleleft K''} \quad \frac{\phi; \Phi \vdash \Delta \sqsubseteq \Delta'; K'' \leq K'}{\phi; \Phi; \Delta \vdash R \triangleleft K'}}{\phi; \Phi; \Delta \vdash (P | Q) | R \triangleleft K'} \quad \frac{\phi; \Phi \vdash \Gamma \sqsubseteq \Delta; K' \leq K}{\phi; \Phi; \Gamma \vdash (P | Q) | R \triangleleft K}$$

The reverse follows the same pattern.

- **Case**  $(\nu a)(\nu b)P \equiv (\nu b)(\nu a)P$ . Suppose  $\phi; \Phi; \Gamma \vdash (\nu a)(\nu b)P \triangleleft K$ . Then the proof has the shape:

$$\frac{\frac{\pi}{\phi; \Phi; \Delta', a : T', b : U \vdash P \triangleleft K''}}{\phi; \Phi; \Delta', a : T' \vdash (\nu b)P \triangleleft K''} \quad \frac{\phi; \Phi \vdash \Delta \sqsubseteq \Delta'; K'' \leq K'; T \sqsubseteq T'}{\phi; \Phi; \Delta, a : T \vdash (\nu b)P \triangleleft K'} \quad \frac{\phi; \Phi \vdash \Gamma \sqsubseteq \Delta; K' \leq K}{\phi; \Phi; \Gamma \vdash (\nu a)(\nu b)P \triangleleft K}$$

We can derive the proof:

$$\frac{\frac{\pi'}{\phi; \Phi; \Delta', a : T', b : U \vdash P \triangleleft K''} \quad \phi; \Phi \vdash T \sqsubseteq T'}{\phi; \Phi; \Delta', a : T, b : U \vdash P \triangleleft K''}}{\phi; \Phi; \Delta', b : U \vdash (\nu a)P \triangleleft K''} \quad \frac{\phi; \Phi \vdash \Gamma \sqsubseteq \Delta'; K'' \leq K}{\phi; \Phi; \Gamma \vdash (\nu b)(\nu a)P \triangleleft K}$$

- **Case**  $(\nu a)P | Q \equiv (\nu a)(P | Q)$  with  $a$  not free in  $Q$ . Suppose  $\phi; \Phi; \Gamma \vdash (\nu a)P | Q \triangleleft K$ . Then the proof has the shape:

$$\frac{\frac{\pi}{\phi; \Phi; \Delta', a : T \vdash P \triangleleft K''}}{\phi; \Phi; \Delta' \vdash (\nu a)P \triangleleft K''} \quad \frac{\phi; \Phi \vdash \Delta \sqsubseteq \Delta'; K'' \leq K'}{\phi; \Phi; \Delta \vdash (\nu a)P \triangleleft K'} \quad \frac{\pi'}{\phi; \Phi; \Delta \vdash Q \triangleleft K'}}{\phi; \Phi; \Delta \vdash (\nu a)P | Q \triangleleft K'} \quad \frac{\phi; \Phi \vdash \Gamma \sqsubseteq \Delta; K' \leq K}{\phi; \Phi; \Gamma \vdash (\nu a)P | Q \triangleleft K}$$

By weakening (Lemma 13), we obtain a proof  $\pi'_w$  of  $\phi; \Phi; \Delta, a : T \vdash Q \triangleleft K'$ . Thus, we have the following derivation:

$$\frac{\frac{\pi}{\phi; \Phi; \Delta', a : T \vdash P \triangleleft K''} \quad \phi; \Phi \vdash \Delta \sqsubseteq \Delta'; T \sqsubseteq T; K'' \leq K'}{\phi; \Phi; \Delta, a : T \vdash P \triangleleft K'} \quad \frac{\pi'_w}{\phi; \Phi; \Delta, a : T \vdash Q \triangleleft K'}
}{\frac{\phi; \Phi; \Delta, a : T \vdash P \mid Q \triangleleft K'}{\phi; \Phi; \Delta \vdash (\nu a)(P \mid Q) \triangleleft K'} \quad \phi; \Phi \vdash \Gamma \sqsubseteq \Delta; K' \leq K}
{\phi; \Phi; \Gamma \vdash (\nu a)(P \mid Q) \triangleleft K}$$

For the converse, suppose  $\phi; \Phi; \Gamma \vdash (\nu a)(P \mid Q) \triangleleft K$ . Then the proof has the shape:

$$\frac{\frac{\pi}{\phi; \Phi; \Delta', a : T' \vdash P \triangleleft K''} \quad \frac{\pi'}{\phi; \Phi; \Delta', a : T' \vdash Q \triangleleft K''}}{\phi; \Phi; \Delta', a : T' \vdash P \mid Q \triangleleft K''} \quad \frac{\phi; \Phi \vdash \Delta \sqsubseteq \Delta'; T \sqsubseteq T'; K'' \leq K'}{\frac{\phi; \Phi; \Delta, a : T \vdash P \mid Q \triangleleft K'}{\phi; \Phi; \Delta \vdash (\nu a)(P \mid Q) \triangleleft K'} \quad \phi; \Phi \vdash \Gamma \sqsubseteq \Delta; K' \leq K}
}{\phi; \Phi; \Gamma \vdash (\nu a)(P \mid Q) \triangleleft K}$$

Since  $a$  is not free in  $Q$ , by Lemma 14, from  $\pi'$  we obtain a proof  $\pi'_c$  of  $\phi; \Phi; \Delta' \vdash Q \triangleleft K''$ . We can then derive the following typing:

$$\frac{\frac{\pi}{\phi; \Phi; \Delta', a : T' \vdash P \triangleleft K''} \quad \phi; \Phi \vdash T \sqsubseteq T'}{\frac{\phi; \Phi; \Delta', a : T \vdash P \triangleleft K''}{\phi; \Phi; \Delta' \vdash (\nu a)P \triangleleft K''}} \quad \frac{\pi'_c}{\phi; \Phi; \Delta' \vdash Q \triangleleft K''}}
{\frac{\phi; \Phi; \Delta' \vdash (\nu a)P \mid Q \triangleleft K''}{\phi; \Phi; \Gamma \vdash (\nu a)P \mid Q \triangleleft K} \quad \phi; \Phi \vdash \Gamma \sqsubseteq \Delta'; K'' \leq K}$$

This concludes all the base case. We can then prove Lemma 18 by induction on  $P \equiv Q$ . All the base case have been done, symmetry and transitivity are direct by induction hypothesis. For the cases of contextual congruence, the proof is again straightforward by considering proofs in which there is exactly one subtyping rule before any syntax-directed rule.  $\square$

Now that we have Lemma 18, we can work up to the congruence relation. We now give an exhaustive description of the subtyping relation.

**Lemma 19** (Exhaustive Description of Subtyping). *If  $\phi; \Phi \vdash T \sqsubseteq U$ , then one of the following case holds.*

- $T = \text{Nat}[I, J] \quad U = \text{Nat}[I', J'] \quad \phi; \Phi \vDash I' \leq I \quad \phi; \Phi \vDash J \leq J'$
- $T = \text{List}[I, J](\mathcal{B}) \quad U = \text{List}[I', J'](\mathcal{B}') \quad \phi; \Phi \vDash I' \leq I \quad \phi; \Phi \vDash J \leq J' \quad \phi; \Phi \vdash \mathcal{B} \sqsubseteq \mathcal{B}'$
- $T = \text{Bool} \quad U = \text{Bool}$
- $T = \text{ch}_I(\tilde{T}) \quad U = \text{ch}_J(\tilde{U}) \quad \phi; \Phi \vDash I = J \quad \phi; \Phi \vdash \tilde{T} \sqsubseteq \tilde{U} \quad \phi; \Phi \vdash \tilde{U} \sqsubseteq \tilde{T}$
- $T = \text{ch}_I(\tilde{T}) \quad U = \text{in}_J(\tilde{U}) \quad \phi; \Phi \vDash I = J \quad \phi; \Phi \vdash \tilde{T} \sqsubseteq \tilde{U}$
- $T = \text{ch}_I(\tilde{T}) \quad U = \text{out}_J(\tilde{U}) \quad \phi; \Phi \vDash I = J \quad \phi; \Phi \vdash \tilde{U} \sqsubseteq \tilde{T}$
- $T = \text{in}_I(\tilde{T}) \quad U = \text{in}_J(\tilde{U}) \quad \phi; \Phi \vDash I = J \quad \phi; \Phi \vdash \tilde{T} \sqsubseteq \tilde{U}$
- $T = \text{out}_I(\tilde{T}) \quad U = \text{out}_J(\tilde{U}) \quad \phi; \Phi \vDash I = J \quad \phi; \Phi \vdash \tilde{U} \sqsubseteq \tilde{T}$

$$\begin{aligned}
& \bullet \\
& T = \forall_{I\tilde{i}}.\text{serv}^K(\tilde{T}) \quad U = \forall_{J\tilde{i}}.\text{serv}^{K'}(\tilde{U}) \quad \phi; \Phi \vDash I = J \quad (\phi, \tilde{i}); \Phi \vdash \tilde{T} \sqsubseteq \tilde{U} \quad (\phi, \tilde{i}); \Phi \vdash \tilde{U} \sqsubseteq \tilde{T} \quad (\phi, \tilde{i}); \Phi \vDash K = K' \\
& \bullet \\
& T = \forall_{I\tilde{i}}.\text{serv}^K(\tilde{T}) \quad U = \forall_{J\tilde{i}}.\text{iserv}^{K'}(\tilde{U}) \quad \phi; \Phi \vDash I = J \quad (\phi, \tilde{i}); \Phi \vdash \tilde{T} \sqsubseteq \tilde{U} \quad (\phi, \tilde{i}); \Phi \vDash K' \leq K \\
& \bullet \\
& T = \forall_{I\tilde{i}}.\text{serv}^K(\tilde{T}) \quad U = \forall_{J\tilde{i}}.\text{oserv}^{K'}(\tilde{U}) \quad \phi; \Phi \vDash I = J \quad (\phi, \tilde{i}); \Phi \vdash \tilde{U} \sqsubseteq \tilde{T} \quad (\phi, \tilde{i}); \Phi \vDash K \leq K' \\
& \bullet \\
& T = \forall_{I\tilde{i}}.\text{iserv}^K(\tilde{T}) \quad U = \forall_{J\tilde{i}}.\text{iserv}^{K'}(\tilde{U}) \quad \phi; \Phi \vDash I = J \quad (\phi, \tilde{i}); \Phi \vdash \tilde{T} \sqsubseteq \tilde{U} \quad (\phi, \tilde{i}); \Phi \vDash K' \leq K \\
& \bullet \\
& T = \forall_{I\tilde{i}}.\text{oserv}^K(\tilde{T}) \quad U = \forall_{J\tilde{i}}.\text{oserv}^{K'}(\tilde{U}) \quad \phi; \Phi \vDash I = J \quad (\phi, \tilde{i}); \Phi \vdash \tilde{U} \sqsubseteq \tilde{T} \quad (\phi, \tilde{i}); \Phi \vDash K \leq K'
\end{aligned}$$

*Proof.* The proof is rather straightforward, we proceed by induction on the subtyping relation. All base cases are indeed of this form, and then for transitivity, we can use the induction hypothesis and consider all cases in which the second member of a subtyping relation can match with the first one, and all cases are simple.  $\square$

Let us now show Theorem 2. We do this by induction on  $P \rightarrow Q$ . Let us first remark that when considering the typing of  $P$ , the first subtyping rule has no importance since we can always start the typing of  $Q$  with the exact same subtyping rule. One can see it in the detailed proof of Lemma 18. We now proceed by doing the case analysis on the rules of Figure 1.

- **Case**  $!a(\tilde{v}).P \mid \bar{a}(\tilde{e}) \rightarrow !a(\tilde{v}).P \mid P[\tilde{v} := \tilde{e}]$ . Consider the typing  $\phi; \Phi; \Gamma \vdash !a(\tilde{v}).P \mid \bar{a}(\tilde{e}) \triangleleft K$ . The first rule is the rule for parallel composition, then the proof is split into the two following subtree:

$$\begin{array}{c}
\frac{\phi; \Phi; \Gamma_1 \vdash a : \forall_{I_1\tilde{i}}.\text{oserv}^{K_1}(\tilde{T}_1) \quad \frac{\pi_e}{\phi; \Phi; \langle \Gamma_1 \rangle_{-I_1} \vdash \tilde{e} : \tilde{T}_1\{\tilde{J}/\tilde{i}\}}}{\phi; \Phi; \Gamma_1 \vdash \bar{a}(\tilde{e}) \triangleleft I_1 + K_1\{\tilde{J}/\tilde{i}\}} \quad \phi; \Phi \vdash \Gamma \sqsubseteq \Gamma_1; I_1 + K_1\{\tilde{J}/\tilde{i}\} \leq K}{\phi; \Phi; \Gamma \vdash \bar{a}(\tilde{e}) \triangleleft K} \\
\\
\frac{\phi; \Phi; \Gamma_0, \Delta_0 \vdash a : \forall_{I_0\tilde{i}}.\text{iserv}^{K_0}(\tilde{T}_0) \quad \frac{\pi_P}{(\phi, \tilde{i}); \Phi; \Gamma', \tilde{v} : \tilde{T}_0 \vdash P \triangleleft K_0} \quad \Gamma' \text{ time invariant} \quad \phi; \Phi \vdash \langle \Gamma_0 \rangle_{-I_0} \sqsubseteq \Gamma'}{\phi; \Phi; \Gamma_0, \Delta_0 \vdash !a(\tilde{v}).P \triangleleft I_0} \quad \phi; \Phi \vdash \Gamma \sqsubseteq \Gamma_0, \Delta_0; I_0 \leq K}{\phi; \Phi; \Gamma \vdash !a(\tilde{v}).P \triangleleft K}
\end{array}$$

The second subtree can be used exactly in the same way to type the server in the right part of the reduction relation. Furthermore, as the name  $a$  is used as an input and as an output, so the original type in  $\Gamma$  for this name must be a server type  $\forall_{I\tilde{i}}.\text{serv}^{K'}(\tilde{T})$ . By Lemma 19, we have:

$$\begin{aligned}
\phi; \Phi \vDash I_0 = I & \quad (\phi, \tilde{i}); \Phi \vdash \tilde{T} \sqsubseteq \tilde{T}_0 & \quad (\phi, \tilde{i}); \Phi \vDash K_0 \leq K' \\
\phi; \Phi \vDash I = I_1 & \quad (\phi, \tilde{i}); \Phi \vdash \tilde{T}_1 \sqsubseteq \tilde{T} & \quad (\phi, \tilde{i}); \Phi \vDash K' \leq K_1
\end{aligned}$$

So, we obtain directly:

$$\phi; \Phi \vDash I_0 = I_1 \quad (\phi, \tilde{i}); \Phi \vdash \tilde{T}_1 \sqsubseteq \tilde{T}_0 \quad (\phi, \tilde{i}); \Phi \vDash K_0 \leq K_1$$

Thus, by subtyping, from  $\pi_P$  we can obtain a proof of  $(\phi, \tilde{i}); \Phi; \langle \Gamma_0 \rangle_{-I_0}, \tilde{v} : \tilde{T}_1 \vdash P \triangleleft K_1$ . By Lemma 15, we have a proof of  $\phi; \Phi\{\tilde{J}/\tilde{i}\}; \langle \Gamma_0 \rangle_{-I_0}, \tilde{v} : \tilde{T}_1\{\tilde{J}/\tilde{i}\} \vdash P \triangleleft K_1\{\tilde{J}/\tilde{i}\}$ . As  $\tilde{i}$  only appears in  $\tilde{T}_1$  and  $K_1$ , we obtain a proof of  $\phi; \Phi; \langle \Gamma_0 \rangle_{-I_0}, \tilde{v} : \tilde{T}_1\{\tilde{J}/\tilde{i}\} \vdash P \triangleleft K_1\{\tilde{J}/\tilde{i}\}$ .

Now, by Lemma 11, we have:

$$\langle \Gamma \rangle_{-I} = \Gamma'_0, \Delta'_0 \quad \phi; \Phi \vdash \Gamma'_0 \sqsubseteq \langle \Gamma_0 \rangle_{-I} \quad \langle \Gamma \rangle_{-I} = \Gamma'_1, \Delta'_1 \quad \phi; \Phi \vdash \Gamma'_1 \sqsubseteq \langle \Gamma_1 \rangle_{-I}$$

By Lemma 13, and as  $\phi; \Phi \vdash I = I_0 = I_1$  we can obtain two proofs:

$$\phi; \Phi; \langle \Gamma_0 \rangle_{-I}, \Delta'_0, \tilde{v} : \tilde{T}_1 \{ \tilde{J} / \tilde{i} \} \vdash P \triangleleft K_1 \{ \tilde{J} / \tilde{i} \} \quad \phi; \Phi; \langle \Gamma_1 \rangle_{-I}, \Delta'_1 \vdash \tilde{e} : \tilde{T}_1 \{ \tilde{J} / \tilde{i} \}$$

Finally, by subtyping, with the remark above, we obtain:

$$\phi; \Phi; \langle \Gamma \rangle_{-I}, \tilde{v} : \tilde{T}_1 \{ \tilde{J} / \tilde{i} \} \vdash P \triangleleft K_1 \{ \tilde{J} / \tilde{i} \} \quad \phi; \Phi; \langle \Gamma \rangle_{-I} \vdash \tilde{e} : \tilde{T}_1 \{ \tilde{J} / \tilde{i} \}$$

Thus, by the substitution lemma (Lemma 17), we have  $\phi; \Phi; \langle \Gamma \rangle_{-I} \vdash P[\tilde{v} := \tilde{e}] \triangleleft K_1 \{ \tilde{J} / \tilde{i} \}$ . Then, by delaying (Lemma 16), we have  $\phi; \Phi; (\langle \Gamma \rangle_{-I})_{+I} \vdash P[\tilde{v} := \tilde{e}] \triangleleft I + K_1 \{ \tilde{J} / \tilde{i} \}$ , and  $\Gamma = \Gamma', \Delta$  with  $\phi; \Phi \vdash \Gamma' \sqsubseteq (\langle \Gamma \rangle_{-I})_{+I}$ . Recall that  $\phi; \Phi \vDash I + K_1 \{ \tilde{J} / \tilde{i} \} \leq K$ . Thus, again by subtyping and weakening, we obtain

$$\phi; \Phi; \Gamma \vdash P[\tilde{v} := \tilde{e}] \triangleleft K$$

And this concludes this case.

- **Case**  $a(\tilde{v}).P \mid \bar{a}(\tilde{e}) \rightarrow P[\tilde{v} := \tilde{e}]$ . Consider the typing  $\phi; \Phi; \Gamma \vdash a(\tilde{v}).P \mid \bar{a}(\tilde{e}) \triangleleft K$ . The first rule is the rule for parallel composition, then the proof is split into the two following subtree:

$$\frac{\frac{\phi; \Phi; \Gamma_1 \vdash a : \text{out}_{I_1}(\tilde{T}_1) \quad \frac{\pi_e}{\phi; \Phi; \langle \Gamma_1 \rangle_{-I_1} \vdash \tilde{e} : \tilde{T}_1}}{\phi; \Phi; \Gamma_1 \vdash \bar{a}(\tilde{e}) \triangleleft I_1} \quad \phi; \Phi \vdash \Gamma \sqsubseteq \Gamma_1; I_1 \leq K}{\phi; \Phi; \Gamma \vdash \bar{a}(\tilde{e}) \triangleleft K}$$

$$\frac{\frac{\phi; \Phi; \Gamma_0 \vdash a : \text{in}_{I_0}(\tilde{T}_0) \quad \frac{\pi_P}{\phi; \Phi; \langle \Gamma_0 \rangle_{-I_0}, \tilde{v} : \tilde{T}_0 \vdash P \triangleleft K_0}}{\phi; \Phi; \Gamma_0 \vdash a(\tilde{v}).P \triangleleft I_0 + K_0} \quad \phi; \Phi \vdash \Gamma \sqsubseteq \Gamma_0; I_0 + K_0 \leq K}{\phi; \Phi; \Gamma \vdash a(\tilde{v}).P \triangleleft K}$$

As the name  $a$  is used as an input and as an output, so the original type in  $\Gamma$  for this name must be a channel type  $\text{ch}_I(\tilde{T})$ . By Lemma 19, we have:

$$\phi; \Phi \vDash I_0 = I \quad \phi; \Phi \vdash \tilde{T} \sqsubseteq \tilde{T}_0 \quad \phi; \Phi \vDash I = I_1 \quad \phi; \Phi \vdash \tilde{T}_1 \sqsubseteq \tilde{T}$$

So, we obtain directly:

$$\phi; \Phi \vDash I_0 = I_1 \quad (\phi, \tilde{i}); \Phi \vdash \tilde{T}_1 \sqsubseteq \tilde{T}_0$$

Thus, by subtyping, from  $\pi_P$  we can obtain a proof of  $\phi; \Phi; \langle \Gamma_0 \rangle_{-I_0}, \tilde{v} : \tilde{T}_1 \vdash P \triangleleft K_0$ . Now, by Lemma 11, we have:

$$\langle \Gamma \rangle_{-I} = \Gamma'_0, \Delta'_0 \quad \phi; \Phi \vdash \Gamma'_0 \sqsubseteq \langle \Gamma_0 \rangle_{-I} \quad \langle \Gamma \rangle_{-I} = \Gamma'_1, \Delta'_1 \quad \phi; \Phi \vdash \Gamma'_1 \sqsubseteq \langle \Gamma_1 \rangle_{-I}$$

By Lemma 13, and as  $\phi; \Phi \vdash I = I_0 = I_1$  we can obtain two proofs:

$$\phi; \Phi; \langle \Gamma_0 \rangle_{-I}, \Delta'_0, \tilde{v} : \tilde{T}_1 \vdash P \triangleleft K_0 \quad \phi; \Phi; \langle \Gamma_1 \rangle_{-I}, \Delta'_1 \vdash \tilde{e} : \tilde{T}_1$$

Then, by subtyping, with the remark above, we obtain:

$$\phi; \Phi; \langle \Gamma \rangle_{-I}, \tilde{v} : \tilde{T}_1 \vdash P \triangleleft K_0 \quad \phi; \Phi; \langle \Gamma \rangle_{-I} \vdash \tilde{e} : \tilde{T}_1$$

Thus, by the substitution lemma (Lemma 17), we have  $\phi; \Phi; \langle \Gamma \rangle_{-I} \vdash P[\tilde{v} := \tilde{e}] \triangleleft K_0$ . Then, by delaying (Lemma 16), we have  $\phi; \Phi; (\langle \Gamma \rangle_{-I})_{+I} \vdash P[\tilde{v} := \tilde{e}] \triangleleft I + K_0$ , and  $\Gamma = \Gamma', \Delta$  with  $\phi; \Phi \vdash \Gamma' \sqsubseteq (\langle \Gamma \rangle_{-I})_{+I}$ . Recall that  $\phi; \Phi \vDash I + K_0 \leq K$ . Thus, again by subtyping and weakening, we obtain

$$\phi; \Phi; \Gamma \vdash P[\tilde{v} := \tilde{e}] \triangleleft K$$

And this concludes this case.

- **Case match  $\square$  with  $\{\square \mapsto P \mid x :: y \mapsto Q\} \rightarrow P$ .** This case is similar to its counterpart for natural number and the two case for booleans, so we only detail this one. Suppose given a derivation  $\phi; \Phi; \Gamma \vdash \text{match } \square \text{ with } \{\square \mapsto P \mid x :: y \mapsto Q\} \triangleleft K$ . Then the derivation has the shape:

$$\frac{\frac{\phi; \Phi; \Delta \vdash \square : \text{List}[0, 0](\mathcal{B}')}{}{\phi; \Phi; \Gamma \vdash \square : \text{List}[I, J](\mathcal{B})} \quad \frac{\phi; \Phi \vdash \Gamma \sqsubseteq \Delta; \text{List}[0, 0](\mathcal{B}') \sqsubseteq \text{List}[I, J](\mathcal{B})}{\phi; \Phi; \Gamma \vdash \square : \text{List}[I, J](\mathcal{B})} \quad \frac{\pi_P}{\phi; (\Phi, I \leq 0); \Gamma \vdash P \triangleleft K} \quad \pi_Q}{\phi; \Phi; \Gamma \vdash \text{match } \square \text{ with } \{\square \mapsto P \mid x :: y \mapsto Q\} \triangleleft K}$$

Where  $\pi_Q$  is the typing for  $Q$  that does not interest us in this case. By Lemma 19, we obtain:

$$\phi; \Phi \models I \leq 0 \quad \phi; \Phi \models 0 \leq J \quad \phi; \Phi \vdash \mathcal{B}' \sqsubseteq \mathcal{B}$$

As  $\phi; \Phi \models I \leq 0$ , by Lemma 14, we obtain directly from  $\pi_P$  a proof  $\phi; \Phi; \Gamma \vdash P \triangleleft K$ .

- **Case match  $e :: e'$  with  $\{\square \mapsto P \mid x :: y \mapsto Q\} \rightarrow Q[x, y := e, e']$ .** This case is more difficult than its counterpart for integers, thus we only detail this case and the one for integers can easily be deduced from this one. Suppose given a derivation  $\phi; \Phi; \Gamma \vdash \text{match } e :: e' \text{ with } \{\square \mapsto P \mid x :: y \mapsto Q\} \triangleleft K$ . Then the proof has the shape:

$$\frac{\frac{\pi_e}{\phi; \Phi; \Delta \vdash e : \mathcal{B}'} \quad \frac{\pi_{e'}}{\phi; \Phi; \Delta \vdash e' : \text{List}[I', J'](\mathcal{B}')}}{\phi; \Phi; \Delta \vdash e :: e' : \text{List}[I' + 1, J' + 1](\mathcal{B}')} \quad \frac{\phi; \Phi \vdash \Gamma \sqsubseteq \Delta; \text{List}[I' + 1, J' + 1](\mathcal{B}') \sqsubseteq \text{List}[I, J](\mathcal{B})}{\phi; \Phi; \Gamma \vdash e :: e' : \text{List}[I, J](\mathcal{B})} \quad \pi_P \quad \pi_Q}{\phi; \Phi; \Gamma \vdash \text{match } e :: e' \text{ with } \{\square \mapsto P \mid x :: y \mapsto Q\} \triangleleft K}$$

Where  $\pi_Q$  is a proof of  $\phi; (\Phi, J \geq 1); \Gamma, x : \mathcal{B}, y : \text{List}[I - 1, J - 1](\mathcal{B}) \vdash Q \triangleleft K$ , and  $\pi_P$  is a typing derivation for  $P$  that does not interest us in this case.

Lemma 19 gives us the following information:

$$\phi; \Phi \models I \leq I' + 1 \quad \phi; \Phi \models J' + 1 \leq J \quad \phi; \Phi \vdash \mathcal{B}' \sqsubseteq \mathcal{B}$$

From this, we can deduce the following constraints:

$$\phi; \Phi \models J \geq 1 \quad \phi; \Phi \models I - 1 \leq I' \quad \phi; \Phi \models J' \leq J - 1$$

Thus, with the subtyping rule and the proofs  $\pi_e$  and  $\pi_{e'}$  we obtain:

$$\phi; \Phi; \Gamma \vdash e : \mathcal{B} \quad \phi; \Phi; \Gamma \vdash e' : \text{List}[I - 1, J - 1](\mathcal{B})$$

Then, by Lemma 14, from  $\pi_Q$  we obtain a proof of  $\phi; \Phi; \Gamma, x : \mathcal{B}, y : \text{List}[I - 1, J - 1](\mathcal{B}) \vdash Q \triangleleft K$ . By the substitution lemma (Lemma 17), we obtain  $\phi; \Phi; \Gamma \vdash Q[x, y := e, e'] \triangleleft K$ . This concludes this case.

- **Case  $P \mid R \rightarrow Q \mid R$  with  $P \rightarrow Q$ .** Suppose that  $\phi; \Phi; \Gamma \vdash P \mid R \triangleleft K$ . Then the proof has the shape:

$$\frac{\frac{\pi_P}{\phi; \Phi; \Gamma \vdash P \triangleleft K} \quad \frac{\pi_R}{\phi; \Phi; \Gamma \vdash R \triangleleft K}}{\phi; \Phi; \Gamma \vdash P \mid R \triangleleft K}$$

By induction hypothesis, with the proof  $\pi_P$  of  $\phi; \Phi; \Gamma \vdash P \triangleleft K$ , we obtain a proof  $\pi_Q$  of  $\phi; \Phi; \Gamma \vdash P \triangleleft Q$ . Then, we can derive the following proof:

$$\frac{\frac{\pi_Q}{\phi; \Phi; \Gamma \vdash P \triangleleft Q} \quad \frac{\pi_R}{\phi; \Phi; \Gamma \vdash R \triangleleft K}}{\phi; \Phi; \Gamma \vdash P \mid R \triangleleft K}$$

This concludes this case.



**Definition 11** (Discarding Deadlocked Processes). *Let  $R$  be a process and  $\mathcal{S}$  a multiset of guarded processes included in the top guarded processes of  $P$  (see the proof of Lemma 2 for a formal definition) such that:*

- $R \equiv (\nu \tilde{a})(P_1 \mid \cdots \mid P_n \mid Q_1 \mid \cdots \mid Q_m)$  with  $P_1, \dots, P_n, Q_1, \dots, Q_m$  guarded processes.
- $[P_1 \dots P_n] = \mathcal{S}$ .
- $\mathcal{S}$  contains only non-replicated input and output processes.
- $P_1 \mid \cdots \mid P_n$  is in normal form for  $\rightarrow$ .
- For each name  $a$  at a top of a process in  $\mathcal{S}$ ,  $a$  cannot appear both at the top of an input process and an output process in  $\mathcal{S}$ .
- There exist  $\Gamma$  such that  $\Gamma \vdash Q_1 \mid \cdots \mid Q_m$  and for each name  $a$  at a top of a process in  $\mathcal{S}$ , either  $a$  appears only at the top of input processes in  $\mathcal{S}$ , and  $a : \text{in}(\tilde{T}) \in \Gamma$  for some  $\tilde{T}$  or  $a$  appears only at the top of output processes in  $\mathcal{S}$ , and  $a : \text{out}(\tilde{T}) \in \Gamma$  for some  $\tilde{T}$ .

Then, we say that  $P'$  is a  $\mathcal{S}$ -discarding of  $P$ , noted  $\text{disc}_{\mathcal{S}}(P, P')$  if  $P' \equiv (\nu \tilde{a})(Q_1 \mid \cdots \mid Q_n)$ .

With this generic notion, we can show that we define a simulation of  $R$  in the following sense.

**Lemma 20.** *If  $R_0 \rightarrow R'_0$  and  $\text{disc}_{\mathcal{S}}(R_0, R_1)$ , then there exists  $R'_1$  such that  $\text{disc}_{\mathcal{S}}(R'_0, R'_1)$  and  $R_1 \rightarrow R'_1$ . We also have the same simulation for  $\Rightarrow$ . Moreover, if  $R_0 \Rightarrow R_0$  and  $\text{disc}_{\mathcal{S}}(R_0, R_1)$  then  $R_1 \Rightarrow R_1$ .*

*Proof.* First, with Lemma 5, we can do a case analysis on the reduction  $R_0 \rightarrow R'_0$ .

- If we are in the case:

$$R_0 \equiv (\nu \tilde{b})(Q_1 \mid \cdots \mid Q_n \mid !a(\tilde{v}).P \mid \bar{a}(\tilde{e})) \quad R'_0 \equiv (\nu \tilde{b})(Q_1 \mid \cdots \mid Q_n \mid !a(\tilde{v}).P \mid P[\tilde{v} := \tilde{e}])$$

By definition of  $\text{disc}_{\mathcal{S}}(R_0, R_1)$ ,  $!a(\tilde{v}).P \notin \mathcal{S}$  because  $\mathcal{S}$  cannot have replicated input. Moreover,  $\bar{a}(\tilde{e}) \notin \mathcal{S}$  since we cannot have  $\Gamma \vdash !a(\tilde{v}).P$  if  $a : \text{out}(\tilde{T}) \in \Gamma$ . So, we can write

$$R_0 \equiv (\nu \tilde{b})(\mathcal{S} \mid Q'_1 \mid \cdots \mid Q'_m \mid !a(\tilde{v}).P \mid \bar{a}(\tilde{e})) \quad R'_0 \equiv (\nu \tilde{b})(\mathcal{S} \mid Q'_1 \mid \cdots \mid Q'_m \mid !a(\tilde{v}).P \mid P[\tilde{v} := \tilde{e}])$$

Now, we want to show that the guarded processes of  $R'_0$  without  $\mathcal{S}$  are typable. By definition of  $\text{disc}_{\mathcal{S}}(R_0, R_1)$ ,  $\Gamma \vdash Q'_1 \mid \cdots \mid Q'_m \mid !a(\tilde{v}).P \mid \bar{a}(\tilde{e})$  with the good restrictions on  $\Gamma$ . By subject reduction of input/output types [13], we obtain directly  $\Gamma \vdash Q'_1 \mid \cdots \mid Q'_m \mid !a(\tilde{v}).P \mid P[\tilde{v} := \tilde{e}]$ . So, if we pose  $R'_1 = (\nu \tilde{b})(Q'_1 \mid \cdots \mid Q'_m \mid !a(\tilde{v}).P \mid P[\tilde{v} := \tilde{e}])$ , we have  $\text{disc}_{\mathcal{S}}(R'_0, R'_1)$  and  $R_1 \rightarrow R'_1$  because:

$$R_1 \equiv (\nu \tilde{b})(Q'_1 \mid \cdots \mid Q'_m \mid !a(\tilde{v}).P \mid \bar{a}(\tilde{e})) \quad R'_1 = (\nu \tilde{b})(Q'_1 \mid \cdots \mid Q'_m \mid !a(\tilde{v}).P \mid P[\tilde{v} := \tilde{e}])$$

- If we are in the case:

$$R_0 \equiv (\nu \tilde{b})(Q_1 \mid \cdots \mid Q_n \mid a(\tilde{v}).P \mid \bar{a}(\tilde{e})) \quad R'_0 \equiv (\nu \tilde{b})(Q_1 \mid \cdots \mid Q_n \mid a(\tilde{v}).P \mid P[\tilde{v} := \tilde{e}])$$

By definition of  $\text{disc}_{\mathcal{S}}(R_0, R_1)$ , either  $a(\tilde{v}).P \notin \mathcal{S}$  or  $\bar{a}(\tilde{e}) \notin \mathcal{S}$  because  $\mathcal{S}$  cannot have a name both at a top of an input and output process. Suppose for example  $a(\tilde{v}).P \notin \mathcal{S}$ . Then,  $\bar{a}(\tilde{e}) \notin \mathcal{S}$  since we cannot have  $\Gamma \vdash a(\tilde{v}).P$  if  $a : \text{out}(\tilde{T}) \in \Gamma$ . Symmetrically, in  $\bar{a}(\tilde{e}) \notin \mathcal{S}$  then  $a(\tilde{v}).P \notin \mathcal{S}$ . So, we can write

$$R_0 \equiv (\nu \tilde{b})(\mathcal{S} \mid Q'_1 \mid \cdots \mid Q'_m \mid a(\tilde{v}).P \mid \bar{a}(\tilde{e})) \quad R'_0 \equiv (\nu \tilde{b})(\mathcal{S} \mid Q'_1 \mid \cdots \mid Q'_m \mid a(\tilde{v}).P \mid P[\tilde{v} := \tilde{e}])$$

Then, we can conclude this proof as in the previous case.

- If we are in the case:

$$R_0 \equiv (\nu \tilde{b})(Q_1 \mid \cdots \mid Q_n \mid \text{match } 0 \text{ with } \{0 \mapsto P \mid \mathfrak{s}(x) \mapsto Q\}) \quad R'_0 \equiv (\nu \tilde{b})(Q_1 \mid \cdots \mid Q_n \mid P)$$

Then by definition,  $\text{match } 0 \text{ with } \{0 \mapsto P \mid \mathfrak{s}(x) \mapsto Q\} \notin \mathcal{S}$ , so we go back to the previous cases where  $\mathcal{S}$  is only in the  $R_i$ . All the other conditionals behaves the same way.

Then, with Lemma 8, we know the shape of a time reduction, and as processes starting with a tick cannot be in  $\mathcal{S}$ , we obtain the result in the same way as conditionals for  $\rightarrow$ . For this, remark that the subject reduction of input/output types for  $\Rightarrow$  is straightforward by definition of the tick rule. Finally, we can prove that if  $R_0 \Rightarrow R_0$  and  $\text{disc}_{\mathcal{S}}(R_0, R_1)$  then  $R_1 \Rightarrow R_1$  by remarking that  $P \Rightarrow P$  if and only if in the top guarded processes of the canonical form of  $P$ , none of them start with a tick.  $\square$

We also show that discarding preserves normal form.

**Lemma 21.** *If  $P$  is in normal form for  $\rightarrow$  and  $\text{disc}_{\mathcal{S}}(P, P')$ , then  $P'$  is in normal form for  $\rightarrow$ .*

*Proof.* With Lemma 5, one can see that if  $\text{disc}_{\mathcal{S}}(P)$  is not in normal form for  $\rightarrow$ , then  $P$  cannot be in normal form, thus we obtain directly the propriety.  $\square$

As a consequence of Lemma 20 and Lemma 21, if a process  $P_0$  can be reduced to  $Q_0$  by the strategy of Definition 3, then, if we have  $\text{disc}_{\mathcal{S}}(P_0, P_1)$ ,  $P_1$  can also be reduced to  $Q_1$  with  $\text{disc}_{\mathcal{S}}(Q_0, Q_1)$  by the same strategy. Indeed, by Lemma 20, when  $P_0 \rightarrow^* P'_0$  then  $P_1 \rightarrow^* P'_1$  with  $\text{disc}_{\mathcal{S}}(P'_0, P'_1)$ , and if  $P'_0$  is in normal form, so is  $P'_1$  by Lemma 21. And then, if  $P'_0 \Rightarrow P'_0$  and the computation stops, then  $P'_1 \Rightarrow P'_1$  and so the computation stops. Otherwise, if  $P'_0 \Rightarrow Q'_0$ , then  $P'_1 \Rightarrow Q'_1$  with  $\text{disc}_{\mathcal{S}}(Q'_0, Q'_1)$ , and we can continue the simulation.

Now, we want to use this with a notion of discarding linked with our type system.

**Definition 12** (Discarding Time Out Processes). *Given a process  $P$  in normal form for  $\rightarrow$  with a proof  $\pi$  of  $\phi; \Phi; \cdot \vdash P \triangleleft K$ , by Lemma 7, its canonical form is:*

$$P \equiv (\nu \tilde{a})(!b_1(\tilde{v}_1^0).P_1 \mid \cdots \mid !b_k(\tilde{v}_k^0).P_k \mid c_1(\tilde{v}_1^1).Q_1 \mid \cdots \mid c_{k'}(\tilde{v}_{k'}^1).Q_{k'} \mid \overline{d_1}(\tilde{e}_1) \mid \cdots \mid \overline{d_{k''}}(\tilde{e}_{k''}) \mid \text{tick}.R_1 \mid \cdots \mid \text{tick}.R_{k'''})$$

with  $(\{b_i \mid 1 \leq i \leq k\} \cup \{c_i \mid 1 \leq i \leq k'\}) \cap \{d_i \mid 1 \leq i \leq k\} = \emptyset$ . In the proof  $\pi$ , a type is given to each name in  $\tilde{a}$  with the rule for the  $(\nu a)$  constructor. Note that during the proof, this type is not fixed because of subtyping, but its time is, as the time of a type is invariant by subtyping. We define the multiset of timed out processes of  $P$  according to  $\pi$ , noted  $\mathcal{T}_{out}^\pi(P)$ , included in the top guarded processes of  $P$  by the following rules:

- A server  $!b_i(\tilde{v}_i^0).P_i$  is never in  $\mathcal{T}_{out}^\pi(P)$ .
- A ticked process  $\text{tick}.R_i$  is never in  $\mathcal{T}_{out}^\pi(P)$ .
- An input  $c_i(\tilde{v}_i^1).Q_i$  is in  $\mathcal{T}_{out}^\pi(P)$  if and only if the time  $I$  of the associated type of  $c_i$  is such that  $\phi; \Phi \not\# I \geq 1$
- An output  $\overline{d_i}(\tilde{e}_i)$  is in  $\mathcal{T}_{out}^\pi(P)$  if and only if the time  $I$  of the associated type of  $d_i$  is such that  $\phi; \Phi \not\# I \geq 1$

When the proof  $\pi$  is not ambiguous, we use  $\mathcal{T}_{out}(P)$ . Now what we want to show is that if  $\text{disc}_{\mathcal{T}_{out}(P)}(P, P')$ , then  $P'$  has exactly the same behaviour as  $P$  for the reductions. In order to do this, we show that  $\mathcal{T}_{out}(P)$  is a special case of Definition 11.

**Lemma 22** (Time Out Processes and Discarding). *Let  $P$  be a process in normal form for  $\rightarrow$  with a proof  $\pi$  of  $\phi; \Phi; \cdot \vdash P \triangleleft K$ . Then,  $\mathcal{T}_{out}(P)$  satisfies the condition of Definition 11.*

*Proof.* First, the fact that  $\mathcal{T}_{out}(P)$  is indeed a multiset of guarded processes included in the top guarded processes of  $P$  is direct. Moreover, by definition,  $\mathcal{T}_{out}(P)$  contains only non-replicated input and output processes, and it is indeed in normal form for  $\rightarrow$ , as  $P$  is in normal form. Now, let us show the two remaining points.

Let  $a$  be a name at a top of a process in  $\mathcal{T}_{out}(P)$ . Suppose that  $a$  appears both at the top of an input process  $a(\tilde{v}).P$  and an output process  $\overline{a}(\tilde{e})$  in  $\mathcal{T}_{out}(P)$ . As  $P$  is typable with sized types, it is also typable without sizes. So, by the usual result on input/output type,  $\tilde{v}$  and  $\tilde{e}$  have the same arity, and base type variables are matched with base type expressions, and channel variable are matched with other channel variables, thus the reduction  $a(\tilde{v}).P \mid \overline{a}(\tilde{e}) \rightarrow P[\tilde{v} := \tilde{e}]$  is defined, which contradicts the fact that  $P$  is in normal form.

Finally, let us consider the canonical form of  $P$ :

$$P \equiv (\nu \tilde{a})(!b_1(\tilde{v}_1^0).P_1 \mid \cdots \mid !b_k(\tilde{v}_k^0).P_k \mid c_1(\tilde{v}_1^1).Q_1 \mid \cdots \mid c_{k'}(\tilde{v}_{k'}^1).Q_{k'} \mid \overline{d_1}(\tilde{e}_1) \mid \cdots \mid \overline{d_{k''}}(\tilde{e}_{k''}) \mid \mathbf{tick}.R_1 \mid \cdots \mid \mathbf{tick}.R_{k'''})$$

with  $(\{b_i \mid 1 \leq i \leq k\} \cup \{c_i \mid 1 \leq i \leq k'\}) \cap \{d_i \mid 1 \leq i \leq k\} = \emptyset$ . By Lemma 18, the typing  $\pi$  of  $P$  gives us a typing of this canonical form. Moreover, in this typing, the name are given the same type as in the original typing  $\pi$  (see the proof of Lemma 18). If we look at the shape of the proof for the canonical form, it starts with rules for  $\nu$  and subtyping rules. And then it uses the rule of parallel composition and again subtyping rules to type each of the guarded processes in the canonical form of  $P$ .

Let us first show that we can always push the subtyping rule in the typing of guarded processes in this case. For this, we show that the rule for subtyping and  $\nu$  can be swapped, and the same for parallel composition.

- If we have the typing:

$$\frac{\frac{\pi}{\phi; \Phi; \Delta, a : T \vdash P \triangleleft K'}}{\phi; \Phi; \Delta \vdash (\nu a)P \triangleleft K'} \quad \phi; \Phi \vDash \Gamma \sqsubseteq \Delta \quad \phi; \Phi \vDash K' \leq K}{\phi; \Phi; \Gamma \vdash (\nu a)P \triangleleft K}$$

Then, we can push the subtyping rule with the following derivation:

$$\frac{\frac{\pi}{\phi; \Phi; \Delta, a : T \vdash P \triangleleft K'} \quad \phi; \Phi \vDash \Gamma, a : T \sqsubseteq \Delta, a : T \quad \phi; \Phi \vDash K' \leq K}{\phi; \Phi; \Gamma, a : T \vdash P \triangleleft K}}{\phi; \Phi; \Gamma \vdash (\nu a)P \triangleleft K}$$

- If we have the typing:

$$\frac{\frac{\pi_P}{\phi; \Phi; \Delta \vdash P \triangleleft K'} \quad \frac{\pi_Q}{\phi; \Phi; \Delta \vdash Q \triangleleft K'}}{\phi; \Phi; \Delta \vdash P \mid Q \triangleleft K'} \quad \phi; \Phi \vDash \Gamma \sqsubseteq \Delta \quad \phi; \Phi \vDash K' \leq K}{\phi; \Phi; \Gamma \vdash P \mid Q \triangleleft K}$$

Then, we can push the subtyping rule with the following derivation:

$$\frac{\frac{\pi_P}{\phi; \Phi; \Delta \vdash P \triangleleft K'} \quad \phi; \Phi \vDash \Gamma \sqsubseteq \Delta \quad \phi; \Phi \vDash K' \leq K}{\phi; \Phi; \Gamma \vdash P \triangleleft K} \quad \frac{\pi_Q}{\phi; \Phi; \Delta \vdash Q \triangleleft K'} \quad \phi; \Phi \vDash \Gamma \sqsubseteq \Delta \quad \phi; \Phi \vDash K' \leq K}{\phi; \Phi; \Gamma \vdash Q \triangleleft K}}{\phi; \Phi; \Gamma \vdash P \mid Q \triangleleft K}$$

As a consequence, by pushing the subtyping rule just before the rule for the typing of guarded processes, we obtain the following derivation for the typing of the canonical form:

$$\frac{\frac{\pi_1, \dots, \pi_n}{\forall i, \phi; \Phi; \tilde{a} : \tilde{U} \vdash S_i \triangleleft K}}{\phi; \Phi; \tilde{a} : \tilde{U} \vdash (S_1 \mid \cdots \mid S_n) \triangleleft K}}{\phi; \Phi; \cdot \vdash (\nu \tilde{a}) \triangleleft (S_1 \mid \cdots \mid S_n)K}$$

Now, we want to show that there exists  $\Gamma'$  (without size types) such that for all guarded process  $S_i \notin \mathcal{T}_{out}(P)$ ,  $\Gamma' \vdash S_i$ , with  $\Gamma'$  giving output type to name in output processes in  $\mathcal{T}_{out}(P)$  and input type to name in input processes in  $\mathcal{T}_{out}(P)$ . We define  $\Gamma' = \tilde{a} : \tilde{U}'$  with:

- If  $U_i = \text{ch}_I(\tilde{T})$  with  $\phi; \Phi \vDash I \geq 1$ , then  $U'_i = \text{ch}(\mathcal{U}(\tilde{T}))$ . (See Definition 10 for  $\mathcal{U}$ ).
- If  $U_i = \text{ch}_I(\tilde{T})$  with  $\phi; \Phi \not\vDash I \geq 1$ , then if  $a_i$  is a top name of a process in  $\mathcal{T}_{out}(P)$ , we pose  $U'_i = \text{in}(\mathcal{U}(\tilde{T}))$  if it appears only at the top of input processes in  $\mathcal{T}_{out}(P)$ , and  $U'_i = \text{out}(\mathcal{U}(\tilde{T}))$  if it only appears at the top of output processes in  $\mathcal{T}_{out}(P)$ . Otherwise, we pose  $U'_i = \text{ch}(\mathcal{U}(\tilde{T}))$
- If  $U_i = \text{in}_I(\tilde{T})$ , then we pose  $U'_i = \text{in}(\mathcal{U}(\tilde{T}))$

- If  $U_i = \text{out}_I(\tilde{T})$ , then we pose  $U'_i = \text{out}(\mathcal{U}(\tilde{T}))$
- If  $U_i = \forall_I \tilde{i}.\text{serv}^K(\tilde{T})$  with  $\phi; \Phi \vDash I \geq 1$ , then  $U'_i = \text{ch}(\mathcal{U}(\tilde{T}))$ .
- If  $U_i = \forall_I \tilde{i}.\text{serv}^K(\tilde{T})$  with  $\phi; \Phi \not\vDash I \geq 1$ , then if  $a_i$  is a top name of a process in  $\mathcal{T}_{\text{out}}(P)$ , we pose  $U'_i = \text{out}(\mathcal{U}(\tilde{T}))$ . (Note that as  $\mathcal{T}_{\text{out}}(P)$  do not contain replicated input,  $a$  can only appear as an output in  $\mathcal{T}_{\text{out}}(P)$ ) Otherwise, we pose  $U'_i = \text{ch}(\mathcal{U}(\tilde{T}))$ .
- If  $U_i = \forall_I \tilde{i}.\text{iserv}^K(\tilde{T})$ , then we pose  $U'_i = \text{in}(\mathcal{U}(\tilde{T}))$ .
- If  $U_i = \forall_I \tilde{i}.\text{oserv}^K(\tilde{T})$ , then we pose  $U'_i = \text{out}(\mathcal{U}(\tilde{T}))$ .

$\Gamma'$  satisfies the restriction of Definition 11. Remark that the only differences between  $\Gamma'$  and  $\mathcal{U}(\tilde{a} : \tilde{U})$  is for names in  $\mathcal{T}_{\text{out}}(P)$  with types that were originally both input and output. Now we need to show that under the context  $\Gamma'$ , all the top guarded processes of  $P$  not in  $\mathcal{T}_{\text{out}}(P)$  can be typed. Let us proceed by case analysis. In order to simplify the notation, we use usual generic notation for the guarded processes instead of the notation specified above.

- If  $!a(\tilde{v}).P$  is a top guarded processes of  $P$ . By definition,  $!a(\tilde{v}).P \notin \mathcal{T}_{\text{out}}(P)$ . Let us consider the typing of  $!a(\tilde{v}).P$ .

$$\frac{\phi; \Phi; \Gamma, \Delta \vdash a : \forall_I \tilde{i}.\text{iserv}^{K'}(\tilde{T}) \quad (\phi, \tilde{i}); \Phi; \Gamma'', \tilde{v} : \tilde{T} \vdash P \triangleleft K' \quad \Gamma'' \text{ time invariant} \quad \phi; \Phi \vdash \langle \Gamma \rangle_{-I}^{\phi; \Phi} \sqsubseteq \Gamma''}{\phi; \Phi; \Gamma, \Delta \vdash !a(\tilde{v}).P \triangleleft I} \quad \frac{\phi; \Phi \vdash \langle \tilde{a} : \tilde{U} \rangle \sqsubseteq \Gamma, \Delta; I \leq K}{\phi; \Phi; \tilde{a} : \tilde{U} \vdash !a(\tilde{v}).P \triangleleft K}$$

As  $\Gamma'$  is time invariant, there is no channel type in  $\Gamma''$ , and all server type must have the shape  $\forall_0 \tilde{i}.\text{oserv}^K(\tilde{T})$  for some  $\tilde{i}, K, \tilde{T}$ . By Lemma 12, we have:

$$\mathcal{U}(\Gamma), \mathcal{U}(\Delta) \vdash a : \text{in}(\mathcal{U}(\tilde{T})) \quad \mathcal{U}(\Gamma''), \tilde{v} : \mathcal{U}(\tilde{T}) \vdash P \quad \mathcal{U}(\Gamma) = \Gamma_0, \Gamma_1 \text{ with } \Gamma_0 \sqsubseteq \mathcal{U}(\Gamma'') \quad \tilde{a} : \mathcal{U}(\tilde{T}) \sqsubseteq \mathcal{U}(\Gamma), \mathcal{U}(\Delta)$$

With weakening, all this could give us a proof of  $\tilde{a} : \mathcal{U}(\tilde{U}) \vdash !a(\tilde{v}).P$ . However, we want a proof of  $\Gamma' \vdash !a(\tilde{v}).P$ . As explained before, the only difference between  $\Gamma'$  and  $\tilde{a} : \mathcal{U}(\tilde{U})$  is for names in  $\mathcal{T}_{\text{out}}(P)$  that were originally both input and output. Let us track the role of those names. For channel name, they are not useful in the typing of  $a$ , as  $a$  is a server, and they do not appear in  $\mathcal{U}(\Gamma'')$  because  $\Gamma''$  is time invariant. Now we only need to work on server name that were originally both input and output but became only output in  $\Gamma'$ . As  $P$  is in normal form,  $\bar{a}(\tilde{e}) \notin \mathcal{T}_{\text{out}}(P)$ . In particular, the server name  $a$  is not a top name in  $\mathcal{T}_{\text{out}}(P)$ . As a consequence, changing the type of server name in  $\mathcal{T}_{\text{out}}(P)$  has no consequence for the typing of  $a$ . Moreover, as  $\Gamma''$  is time invariant, changing input and output servers type to output types has no consequence for the typing of  $P$ . So, in the end, we have indeed  $\Gamma' \vdash !a(\tilde{v}).P$ .

- If  $a(\tilde{v}).P$  is a top guarded processes of  $P$  not in  $\mathcal{T}_{\text{out}}(P)$ . Let us consider the typing of  $a(\tilde{v}).P$ .

$$\frac{\phi; \Phi; \Gamma \vdash a : \text{in}_I(\tilde{T}) \quad \phi; \Phi; \langle \Gamma \rangle_{-I} \vdash P \triangleleft K'}{\phi; \Phi; \Gamma \vdash a(\tilde{v}).P \triangleleft I + K'} \quad \frac{\phi; \Phi \vdash \tilde{a} : \tilde{U} \sqsubseteq \Gamma; I + K' \leq K}{\phi; \Phi; \tilde{a} : \tilde{U} \vdash a(\tilde{v}).P \triangleleft K}$$

By Lemma 12, we have:

$$\mathcal{U}(\Gamma) \vdash a : \text{in}(\mathcal{U}(\tilde{T})) \quad \mathcal{U}(\Gamma) = \mathcal{U}(\langle \Gamma \rangle_{-I}), \Delta \quad \mathcal{U}(\langle \Gamma \rangle_{-I}) \vdash P \quad \tilde{a} : \mathcal{U}(\tilde{T}) \sqsubseteq \mathcal{U}(\Gamma)$$

So, by weakening we obtain a proof  $\tilde{a} : \mathcal{U}(\tilde{U}) \vdash a(\tilde{v}).P$ . Again, we want a proof of  $\Gamma' \vdash a(\tilde{v}).P$ . As  $a(\tilde{v}).P \notin \mathcal{T}_{\text{out}}(P)$ , we have  $\phi; \Phi \vDash I \geq 1$ . As a consequence, the typing of  $a$  is not modified in  $\Gamma'$ . Moreover, all time out channels are erased in  $\langle \Gamma \rangle_{-I}$ , so they have no incidence on the typing. Finally, the timed out input/output server names are changed to output server names by  $\langle \Gamma \rangle_{-I}$ , thus we have indeed  $\Gamma' \vdash a(\tilde{v}).P$ .

- If  $\bar{a}(\tilde{e})$  is a top guarded processes of  $P$  not in  $\mathcal{T}_{\text{out}}(P)$ . There are two cases,  $a$  is a channel name or  $a$  is a server name. In both cases, the proof has the same reasoning as the one for  $a(\tilde{v}).P$ .

- If  $\text{tick}.P$  is a top guarded processes of  $P$ . By definition,  $\text{tick}.P \notin \mathcal{T}_{out}(P)$ . Then, the proof has the same reasoning as the one for  $a(\tilde{v}).P$ .

This concludes the proof of Lemma 22.  $\square$

As a consequence, when given a typed process  $P$  is normal form, we can define  $\mathcal{S} = \mathcal{T}_{out}(P)$  and we now that if  $\text{disc}_{\mathcal{S}}(P, P')$ , then  $P'$  can simulate the strategy of Definition 3 on  $P$ .

Now we want to show the following theorem:

**Theorem 3** (Quantitative Subject Reduction). *If  $P$  is in normal form for  $\rightarrow$ ,  $P \Rightarrow Q$  with  $Q \neq P$  and  $\phi; \Phi; \cdot \vdash P \triangleleft K$  then, if we pose  $\mathcal{S} = \mathcal{T}_{out}(P)$ , we have  $\phi; \Phi; \cdot \vdash Q' \triangleleft K'$  with  $\text{disc}_{\mathcal{S}}(Q, Q')$  and  $\phi; \Phi \vDash K' + 1 \leq K$ .*

*Proof.* By Lemma 7, we know the canonical form of  $P$ . As  $P \Rightarrow Q$  with  $Q \neq P$ , we know that  $P$  has at least one top guarded process starting with a  $\text{tick}$ . Let us write:

$$P \equiv (\nu \tilde{a})(\mathcal{T}_{out}(P) \mid P_1 \mid \cdots \mid P_n \mid \text{tick}.R_1 \mid \cdots \mid \text{tick}.R_m)$$

With  $m \geq 1$ . Then, let us pose:

$$Q' = (\nu \tilde{a})(P_1 \mid \cdots \mid P_n \mid R_1 \mid \cdots \mid R_m)$$

By Lemma 8, we have:

$$Q \equiv (\nu \tilde{a})(\mathcal{T}_{out}(P) \mid P_1 \mid \cdots \mid P_n \mid R_1 \mid \cdots \mid R_m)$$

Thus, we have indeed  $\text{disc}_{\mathcal{S}}(Q, Q')$  by Lemma 22. Now, let us consider the typing for the canonical form of  $P$  to give a typing for  $Q'$ . As previously, we consider that subtyping have been pushed to the typing of guarded processes.

$$\frac{\frac{\phi; \Phi; \tilde{a} : \tilde{U} \vdash \mathcal{T}_{out}(P) \triangleleft K \quad \forall i, \phi; \Phi; \tilde{a} : \tilde{U} \vdash P_i \triangleleft K \quad \forall j, \phi; \Phi; \tilde{a} : \tilde{U} \vdash \text{tick}.R_j \triangleleft K}{\phi; \Phi; \tilde{a} : \tilde{U} \vdash (\mathcal{T}_{out}(P) \mid P_1 \mid \cdots \mid P_n \mid \text{tick}.R_1 \mid \cdots \mid \text{tick}.R_m) \triangleleft K}}{\phi; \Phi; \cdot \vdash (\nu \tilde{a})(\mathcal{T}_{out}(P) \mid P_1 \mid \cdots \mid P_n \mid \text{tick}.R_1 \mid \cdots \mid \text{tick}.R_m) \triangleleft K}$$

First, we can see that because of the rule for  $\text{tick}$ , we have  $\phi; \Phi \vDash K \geq 1$ . So, we will show that  $\phi; \Phi; \cdot \vdash Q' \triangleleft K - 1$ , and we have indeed  $\phi; \Phi \vDash (K - 1) + 1 \leq K$ . (Note that if  $K = 0$  this last inequation is not true, that is why we first need  $\phi; \Phi \vDash K \geq 1$ ). In order to do this, let us decide a new assignment to the name in  $\tilde{a}$ . In order to do this, we take the assignment  $\tilde{a} : \tilde{U}$  and we apply the following function on  $\tilde{U}$ :

- $\text{ch}_I(\tilde{T}) \mapsto \text{ch}_{(I-1)}(\tilde{T})$ . Other channel types follow exactly the same pattern.
- $\forall_{I \tilde{i}} \text{serv}^K(\tilde{T}) \mapsto \forall_{(I-1) \tilde{i}} \text{serv}^K(\tilde{T})$ . Other server types follow exactly the same pattern.

We denote this new assignment by  $\tilde{a} : \tilde{U}'$ . Remark that we have  $\tilde{a} : \tilde{U}' = \Gamma', \Delta'$  with the subtyping  $\phi; \Phi \vdash \Gamma' \sqsubseteq \langle \langle \tilde{a} : \tilde{U} \rangle \rangle_{-1}$ . Note also that we have the following lemma:

**Lemma 23.**  $\langle \Gamma \rangle_{-I} = \langle \langle \Gamma \rangle_{-1} \rangle_{-(I-1)}$  when  $\phi; \Phi \vDash I \geq 1$ .

The proof is simple as when  $\phi; \Phi \vDash I \geq 1$ , we have  $\phi; \Phi \vDash J \geq I \Leftrightarrow \phi; \Phi \vDash J \geq 1 \wedge (J - 1) \geq (I - 1)$ . Now, let us give a typing for  $Q'$ .

$$\frac{\frac{\forall i, \phi; \Phi; \tilde{a} : \tilde{U}' \vdash P_i \triangleleft K - 1 \quad \forall j, \phi; \Phi; \tilde{a} : \tilde{U}' \vdash R_j \triangleleft K - 1}{\phi; \Phi; \tilde{a} : \tilde{U}' \vdash (P_1 \mid \cdots \mid P_n \mid R_1 \mid \cdots \mid R_m) \triangleleft K - 1}}{\phi; \Phi; \cdot \vdash (\nu \tilde{a})(P_1 \mid \cdots \mid P_n \mid R_1 \mid \cdots \mid R_m) \triangleleft K - 1}$$

Where the proofs for the  $P_i$  are:

- If  $P_i = !a(\tilde{v}).P$ . Then, the original proof for the canonical form of  $P$  was:

$$\frac{\phi; \Phi; \Gamma, \Delta \vdash a : \forall_{\tilde{I}} \tilde{i}. \text{iserv}^{K'}(\tilde{T}) \quad (\phi, \tilde{i}); \Phi; \Gamma'', \tilde{v} : \tilde{T} \vdash P \triangleleft K' \quad \Gamma'' \text{ time invariant} \quad \phi; \Phi \vdash \langle \Gamma \rangle_{-\tilde{I}}^{\phi; \Phi} \sqsubseteq \Gamma''}{\frac{\phi; \Phi; \Gamma, \Delta \vdash !a(\tilde{v}).P \triangleleft I}{\phi; \Phi; \tilde{a} : \tilde{U} \vdash !a(\tilde{v}).P \triangleleft K} \quad \phi; \Phi \vdash \langle \tilde{a} : \tilde{U} \rangle \sqsubseteq \Gamma, \Delta; I \leq K}}$$

Then, an easy case to consider is when  $\phi; \Phi \models I \geq 1$ . In this case, we can give the following typing, by using previous remarks, Lemma 11 and Lemma 23. Indeed, Lemma 11 gives us:

$$\langle \tilde{a} : \tilde{U} \rangle_{-1} = \Gamma_0, \Delta'' \text{ with } \phi; \Phi \vdash \Gamma_0 \sqsubseteq \langle \Gamma \rangle_{-1}, \langle \Delta \rangle_{-1}$$

and so we obtain the following proof (without recalling the subtyping):

$$\frac{\phi; \Phi; \langle \Gamma \rangle_{-1}, \langle \Delta \rangle_{-1}, \Delta', \Delta'' \vdash a : \forall_{\langle \Gamma \rangle_{-1}} \tilde{i}. \text{iserv}^{K'}(\tilde{T}) \quad (\phi, \tilde{i}); \Phi; \Gamma'', \tilde{v} : \tilde{T} \vdash P \triangleleft K' \quad \Gamma'' \text{ time invariant} \quad \phi; \Phi \vdash \langle \Gamma \rangle_{-\tilde{I}}^{\phi; \Phi} \sqsubseteq \Gamma''}{\frac{\phi; \Phi; \langle \Gamma \rangle_{-1}, \langle \Delta \rangle_{-1}, \Delta', \Delta'' \vdash !a(\tilde{v}).P \triangleleft I - 1}{\frac{\phi; \Phi; \langle \tilde{a} : \tilde{U} \rangle_{-1}, \Delta' \vdash !a(\tilde{v}).P \triangleleft K - 1}{\phi; \Phi; \Gamma', \Delta' \vdash !a(\tilde{v}).P \triangleleft K - 1}}}}$$

Now we need to consider the more difficult case  $\phi; \Phi \not\models I \geq 1$ . Let us consider that type  $T$  assigned to  $a$  in  $\tilde{a} : \tilde{U}$ . By Lemma 19, as  $\phi; \Phi \vdash T \sqsubseteq \forall_{\tilde{I}} \tilde{i}. \text{iserv}^{K'}(\tilde{T})$  we have:

$$T = \forall_{\tilde{J}} \tilde{i}. \text{serv}^{K''}(\tilde{T}') \quad \phi; \Phi \models I = J \quad (\phi, \tilde{i}); \Phi \vdash \tilde{T}' \sqsubseteq \tilde{T} \quad (\phi, \tilde{i}); \Phi \models K' \leq K''$$

or,

$$T = \forall_{\tilde{J}} \tilde{i}. \text{iserv}^{K''}(\tilde{T}') \quad \phi; \Phi \models I = J \quad (\phi, \tilde{i}); \Phi \vdash \tilde{T}' \sqsubseteq \tilde{T} \quad (\phi, \tilde{i}); \Phi \models K' \leq K''$$

In both cases, we can see that the type  $T'$  assigned to  $a$  in  $\tilde{a} : \tilde{U}'$  is such that we have the subtyping  $\phi; \Phi \vdash T' \sqsubseteq \forall_{\langle \Gamma \rangle_{-1}} \tilde{i}. \text{iserv}^{K'}(\tilde{T})$

Now, let us look at what happens to server name in  $\Gamma''$  the original proof for the canonical form of  $P$ . For all axiom  $b : \forall_0 \tilde{i}. \text{oserv}^K(\tilde{T})$  in  $\Gamma''$ , we have  $b : T \in \tilde{a} : \tilde{U}$  such that:

$$\phi; \Phi \vdash T \sqsubseteq T' \quad \phi; \Phi \vdash \langle T' \rangle_{-I} \sqsubseteq \forall_{\tilde{I}} \tilde{i}. \text{oserv}^K(\tilde{T})$$

So, with Lemma 19, we have:

$$\langle T' \rangle_{-I} = \forall_{\tilde{J}} \tilde{i}. \text{serv}^{K'}(\tilde{T}') \quad \phi; \Phi \models J = 0 \quad (\phi, \tilde{i}); \Phi \vdash \tilde{T} \sqsubseteq \tilde{T}' \quad (\phi, \tilde{i}); \Phi \models K' \leq K$$

or

$$\langle T' \rangle_{-I} = \forall_{\tilde{J}} \tilde{i}. \text{oserv}^{K'}(\tilde{T}') \quad \phi; \Phi \models J = 0 \quad (\phi, \tilde{i}); \Phi \vdash \tilde{T} \sqsubseteq \tilde{T}' \quad (\phi, \tilde{i}); \Phi \models K' \leq K$$

Then, by Definition 8, this gives the following possibilities:

$$T' = \forall_{\langle \Gamma \rangle_{-I}} \tilde{i}. \text{serv}^{K'}(\tilde{T}') \quad \phi; \Phi \models J = 0 \quad (\phi, \tilde{i}); \Phi \vdash \tilde{T} \sqsubseteq \tilde{T}' \quad (\phi, \tilde{i}); \Phi \models K' \leq K$$

or

$$T' = \forall_{\tilde{J}'} \tilde{i}. \text{serv}^{K'}(\tilde{T}') \quad \phi; \Phi \not\models J' \geq I \quad \phi; \Phi \models J' - I = 0 \quad (\phi, \tilde{i}); \Phi \vdash \tilde{T} \sqsubseteq \tilde{T}' \quad (\phi, \tilde{i}); \Phi \models K' \leq K$$

or

$$T' = \forall_{\tilde{J}'} \tilde{i}. \text{oserv}^{K'}(\tilde{T}') \quad \phi; \Phi \models J' - I = 0 \quad (\phi, \tilde{i}); \Phi \vdash \tilde{T} \sqsubseteq \tilde{T}' \quad (\phi, \tilde{i}); \Phi \models K' \leq K$$

Note that the two first case can be combined by a type with a time  $J'$  such that  $\phi; \Phi \models J' - I = 0$ . Then, we can use again Lemma 5, and we obtain:

$$T = \forall_{\tilde{J}''} \tilde{i}. \text{serv}^{K''}(\tilde{T}'') \quad \phi; \Phi \models J'' - I = 0 \quad (\phi, \tilde{i}); \Phi \vdash \tilde{T} \sqsubseteq \tilde{T}'' \quad (\phi, \tilde{i}); \Phi \models K'' \leq K$$

or

$$T = \forall_{\tilde{J}''} \tilde{i}. \text{oserv}^{K''}(\tilde{T}'') \quad \phi; \Phi \models J'' - I = 0 \quad (\phi, \tilde{i}); \Phi \vdash \tilde{T} \sqsubseteq \tilde{T}'' \quad (\phi, \tilde{i}); \Phi \models K'' \leq K$$

So, in the assignment  $\tilde{a} : \tilde{U}'$ , this type  $T$  is sent to a type  $T_{new}$  corresponding to  $T$  with a time  $J'' - 1$  instead of  $J''$ . It is easy to see that in both cases, we have  $\phi; \Phi \vdash \langle T_{new} \rangle_{-I} \sqsubseteq \forall_0 \tilde{a}. \text{oserv}^K(\tilde{T})$ . So, we can write  $\tilde{a} : \tilde{U}' = \Gamma_1, \Delta_1$  with  $\phi; \Phi \vdash \langle \Gamma_1 \rangle_{-I} \sqsubseteq \Gamma''$ . And we obtain the following typing:

$$\frac{\phi; \Phi; \Gamma_1, \Delta_1 \vdash a : \forall_{(I-1)} \tilde{a}. \text{iserv}^{K'}(\tilde{T}) \quad (\phi, \tilde{v}); \Phi; \Gamma'', \tilde{v} : \tilde{T} \vdash P \triangleleft K' \quad \Gamma'' \text{ time invariant} \quad \phi; \Phi \vdash \langle \Gamma_1 \rangle_{-I} \sqsubseteq \Gamma''}{\frac{\phi; \Phi; \Gamma_1, \Delta_1 \vdash !a(\tilde{v}).P \triangleleft I - 1}{\phi; \Phi; \Gamma_1, \Delta_1 \vdash !a(\tilde{v}).P \triangleleft K - 1}}$$

This concludes this case.

- If  $P_i = a(\tilde{v}).P$ . Then, the original proof for the canonical form of  $P$  was:

$$\frac{\phi; \Phi; \Gamma \vdash a : \text{in}_I(\tilde{T}) \quad \phi; \Phi; \langle \Gamma \rangle_{-I}, \tilde{v} : \tilde{T} \vdash P \triangleleft K'}{\frac{\phi; \Phi; \Gamma \vdash !a(\tilde{v}).P \triangleleft I + K' \quad \phi; \Phi \vdash \langle \tilde{a} : \tilde{U} \rangle \sqsubseteq \Gamma; I + K' \leq K}{\phi; \Phi; \tilde{a} : \tilde{U} \vdash a(\tilde{v}).P \triangleleft K}}$$

As  $P_i \notin \mathcal{T}_{out}(P)$ , we have  $\phi; \Phi \vdash I \geq 1$ . We can give the following typing, by using previous remarks, Lemma 11 and Lemma 23. Indeed, Lemma 11 gives us:

$$\langle \langle \tilde{a} : \tilde{U} \rangle \rangle_{-1} = \Gamma_0, \Delta'' \text{ with } \phi; \Phi \vdash \Gamma_0 \sqsubseteq \langle \Gamma \rangle_{-1}$$

and so we obtain the following proof (without recalling the subtyping):

$$\frac{\frac{\phi; \Phi; \langle \Gamma \rangle_{-1}, \Delta', \Delta'' \vdash a : \text{in}_{(I-1)}(\tilde{T}) \quad \phi; \Phi; \langle \Gamma \rangle_{-I}, \tilde{v} : \tilde{T} \vdash P \triangleleft K'}{\phi; \Phi; \langle \Gamma \rangle_{-1}, \Delta', \Delta'' \vdash a(\tilde{v}).P \triangleleft (I-1) + K'}}{\frac{\phi; \Phi; \langle \langle \tilde{a} : \tilde{U} \rangle \rangle_{-1}, \Delta' \vdash a(\tilde{v}).P \triangleleft K - 1}{\phi; \Phi; \Gamma', \Delta' \vdash a(\tilde{v}).P \triangleleft K - 1}}$$

- If  $P_i = \bar{a}(\tilde{e})$ , then we can do as the previous case for  $a(\tilde{v}).P$ .

Then, we need to type  $R_j$ . By the remark that  $\tilde{a} : \tilde{U}'$  can be written  $\Gamma', \Delta'$  with the subtyping  $\phi; \Phi \vdash \Gamma' \sqsubseteq \langle \langle \tilde{a} : \tilde{U} \rangle \rangle_{-1}$ , then it can be done by weakening and subtyping. This concludes the proof for Theorem 3.  $\square$

## 4.4 Complexity Bound

This short section is to prove the main theorem of this paper.

**Theorem 4.** *If  $\phi; \Phi; \cdot \vdash P \triangleleft K$  and  $P$  reduces to  $Q$  by the strategy of Definition 3 with  $n$  time reductions, then  $\phi; \Phi \vdash K \geq n$ .*

*Proof.* We prove the following lemma:

**Lemma 24.** *For all integer  $n$ , for all set of constraints  $\Phi$  over  $\phi$ , for all index  $K$ , for all processes  $P, Q$ , if  $\phi; \Phi; \cdot \vdash P \triangleleft K$  and  $P$  can be reduced to  $Q$  by the strategy of Definition 3 with  $n$  time reductions, then  $\phi; \Phi \vdash K \geq n$ .*

By induction on  $n$ .

- **Case  $n = 0$ .** For any  $\phi, \Phi, K$ , we have  $\phi; \Phi \vdash K \geq 0$ , so we obtain directly this case.
- **Case  $n + 1$ .** By Definition 3, we have  $P \rightarrow^* P'$  with  $P'$  in normal form for  $\rightarrow$ . Moreover,  $P' \Rightarrow P_0$ , with  $P_1 \neq P'$  and  $P_1$  can be reduced to  $Q$  by the strategy of Definition 3 with  $n$  time reductions. By hypothesis, we have  $\phi; \Phi; \cdot \vdash P \triangleleft K$ . By Theorem 2, we have  $\phi; \Phi; \cdot \vdash P' \triangleleft K$ . By Theorem 3, if we pose  $S = \mathcal{T}_{out}(P')$ , we have  $\phi; \Phi; \cdot \vdash P_1 \triangleleft K'$  with  $\text{disc}_S(P_0, P_1)$  and  $\phi; \Phi \vdash K' + 1 \leq K$ .

By Lemma 20 and Lemma 21, there exists  $Q_1$  such that  $\text{disc}_S(Q, Q_1)$  and  $P_1$  can be reduced to  $Q_1$  by the strategy with  $n$  time reductions. By induction hypothesis, we obtain  $\phi; \Phi \vdash K' \geq n$ . Thus,  $\phi; \Phi \vdash K \geq K' + 1 \geq n + 1$ . This concludes the proof.  $\square$

So we have indeed that the typing of a process can give a bound on its complexity under maximal parallelism.

```

!merge( $l_0, l_1, a$ ). match  $l_0$  with
| []  $\mapsto \bar{a}\langle l_1 \rangle$ 
|  $x :: q \mapsto$  match  $l_1$  with
| []  $\mapsto \bar{a}\langle l_0 \rangle$ 
|  $y :: r \mapsto (\nu b)(\text{tick}.\overline{\text{compare}}\langle x, y, b \rangle \mid b(z). \text{if } z \text{ then}$ 
   $(\nu c)(\overline{\text{merge}}\langle q, l_1, c \rangle \mid c(l_2).\bar{a}\langle x :: l_2 \rangle)$  else
   $(\nu c)(\overline{\text{merge}}\langle l_0, r, c \rangle \mid c(l_2).\bar{a}\langle y :: l_2 \rangle)$ 
)

!decompose( $l, a_0, a_1$ ). match  $l$  with
| []  $\mapsto \bar{a}_0\langle [] \rangle \mid \bar{a}_1\langle [] \rangle$ 
|  $x :: q \mapsto$  match  $q$  with
| []  $\mapsto \bar{a}_0\langle x :: [] \rangle \mid \bar{a}_1\langle [] \rangle$ 
|  $y :: r \mapsto (\nu b_0)(\nu b_1).(\overline{\text{decompose}}\langle r, b_0, b_1 \rangle \mid b_0(l_0).\bar{a}_0\langle x :: l_0 \rangle \mid b_1(l_1).\bar{a}_1\langle y :: l_1 \rangle)$ 

!mergesort( $l, a$ ). match  $l$  with
| []  $\mapsto \bar{a}\langle [] \rangle$ 
|  $x :: q \mapsto$  match  $q$  with
| []  $\mapsto \bar{a}\langle x :: [] \rangle$ 
|  $y :: r \mapsto (\nu b_0)(\nu b_1)(\nu c_0)(\nu c_1)(\nu d)(\overline{\text{decompose}}\langle l, b_0, b_1 \rangle$ 
   $\mid b_0(l_0).\text{mergesort}\langle l_0, c_0 \rangle \mid b_1(l_1).\text{mergesort}\langle l_1, c_1 \rangle$ 
   $\mid c_0(q_0).c_1(q_1).\overline{\text{merge}}\langle q_0, q_1, d \rangle \mid d(q_2).\bar{a}\langle q_2 \rangle$ 
)

```

Figure 9: Merge Sort

## 5 Examples

We present here an example for this complexity, showing that under maximal parallelism, merge sort has a linear number of comparison. Suppose given a replicated input with name *compare* doing the comparison between two elements of type  $\mathcal{B}$ . We want to count the number of comparison in merge sort. The processes are described in Figure 9.

We now describe the typing for those processes. To take in account the complexity of the comparison, we do a tick before each call to compare, and we give this server the type  $\forall_0.\text{serv}^0(\mathcal{B}, \mathcal{B}, \text{out}_0(\text{Bool}))$ . Note that we could have equivalently given a complexity 1 to the server and removed the tick. In order to simplify the notation, we bound the sizes of the lists in mergesort by an exponent of 2. Let us pose the following context:

$$\Gamma := \text{compare} : \forall_0.\text{serv}^0(\mathcal{B}, \mathcal{B}, \text{out}_0(\text{Bool})), \text{merge} : \forall_0(i, j).\text{serv}^{i+j}(\text{List}[0, i](\mathcal{B}), \text{List}[0, j](\mathcal{B}), \text{out}_{i+j}(\text{List}[0, i+j](\mathcal{B}))),$$

$$\text{decompose} : \forall_0 i.\text{serv}^0(\text{List}[0, 2i](\mathcal{B}), \text{out}_0(\text{List}[0, i](\mathcal{B})), \text{out}_0(\text{List}[0, i](\mathcal{B}))),$$

$$\text{mergesort} : \forall_0 i.\text{serv}^{2^{i+1}}(\text{List}[0, 2^i](\mathcal{B}), \text{out}_{2^{i+1}}(\text{List}[0, 2^i](\mathcal{B})))$$

And we pose  $\Gamma_o$  the same context with output server instead of input/output, thus  $\Gamma_o$  is time unlimited, and we have  $\cdot \vdash \Gamma \sqsubseteq \Gamma_o$ . Moreover,  $\langle \Gamma \rangle_{-o} = \Gamma$ .

We want to show that the servers are well typed under this context. In the typing, we omit the typing of expressions when it is obvious, that is to say only syntax directed rule or a subtyping where an input/output becomes only input or only output without changing anything else.

We start with the server for merge. We pose:

$$\Gamma' := \Gamma_o, l_0 : \text{List}[0, i](\mathcal{B}), l_1 : \text{List}[0, j](\mathcal{B}), a : \text{out}_{i+j}(\text{List}[0, i+j](\mathcal{B}))$$

$$\Gamma'' := \Gamma', x : \mathcal{B}, q : \text{List}[0, i-1](\mathcal{B}), y : \mathcal{B}, r : \text{List}[0, j-1](\mathcal{B})$$

$$\begin{array}{c}
\frac{}{(i, j); (i \geq 1, j \geq 1); \langle \Gamma'' \rangle_{-1}, b : \text{out}_0(\text{Bool}) \vdash \overline{\text{compare}}(x, y, b) \triangleleft 0} \\
\frac{}{(i, j); (i \geq 1, j \geq 1); \Gamma'', b : \text{out}_1(\text{Bool}) \vdash \text{tick}.\overline{\text{compare}}(x, y, b) \triangleleft 1} \\
\frac{}{(i, j); (i \geq 1, j \geq 1); \Gamma'', b : \text{ch}_1(\text{Bool}) \vdash \text{tick}.\overline{\text{compare}}(x, y, b) \triangleleft i + j} \quad \pi \\
\frac{}{(i, j); (i \geq 1, j \geq 1); \Gamma'', b : \text{ch}_1(\text{Bool}) \vdash \text{tick}.\overline{\text{compare}}(x, y, b) \mid b(z) \cdots \triangleleft i + j} \\
\frac{}{(i, j); (i \geq 1, j \geq 1); \Gamma'' \vdash (\nu b)(\text{tick}.\overline{\text{compare}}(x, y, b) \mid b(z) \cdots) \triangleleft i + j} \\
\frac{}{(i, j); 0 \leq 0; \Gamma' \vdash \overline{a}(l_1) \triangleleft i + j} \quad \frac{}{(i, j); (i \geq 1); \Gamma', x : \mathcal{B}, q : \text{List}[0, i - 1](\mathcal{B}) \vdash \text{match } l_1 \text{ with } \{\square \mapsto \overline{a}(l_1) \mid y :: r \mapsto \cdots\} \triangleleft i + j} \\
\frac{}{(i, j); \cdot; \Gamma' \vdash \text{match } l_0 \text{ with } \{\square \mapsto \overline{a}(l_1) \mid x :: q \mapsto \cdots\} \triangleleft i + j} \\
\cdot; \Gamma \vdash !\text{merge}(l_0, l_1, a) \cdots \triangleleft 0
\end{array}$$

where  $\pi$  is the following proof, in which we pose:

$$\begin{aligned}
\Delta &= \Gamma_o, l_0 : \text{List}[0, i](\mathcal{B}), l_1 : \text{List}[0, j](\mathcal{B}), a : \text{out}_{i+j-1}(\text{List}[0, i + j](\mathcal{B})), \\
x : \mathcal{B}, q : \text{List}[0, i - 1](\mathcal{B}), y : \mathcal{B}, r : \text{List}[0, j - 1](\mathcal{B}), b : \text{ch}_0(\text{Bool}), z : \text{Bool} \\
\Delta' &= \Delta, c : \text{ch}_{i+j-1}(\text{List}[0, i + j - 1](\mathcal{B})) \\
\Delta'' &= \langle \Delta' \rangle_{-(i+j-1)}, l_2 : \text{List}[0, i + j - 1](\mathcal{B})
\end{aligned}$$

$$\begin{array}{c}
\frac{}{(i, j); (i \geq 1, j \geq 1); \Delta' \vdash \overline{\text{merge}}(q, l_1, c) \triangleleft i + j - 1} \quad \frac{}{(i, j); (i \geq 1, j \geq 1); \Delta'' \vdash \overline{a}(x :: l_2) \triangleleft 0} \\
\frac{}{(i, j); (i \geq 1, j \geq 1); \Delta, c : \text{ch}_{i+j-1}(\text{List}[0, i + j - 1](\mathcal{B})) \vdash \overline{\text{merge}}(q, l_1, c) \mid c(l_2).\overline{a}(x :: l_2) \triangleleft i + j - 1} \\
\frac{}{(i, j); (i \geq 1, j \geq 1); \Delta \vdash (\nu c)(\overline{\text{merge}}(q, l_1, c) \mid c(l_2).\overline{a}(x :: l_2)) \triangleleft i + j - 1} \quad \cdots \\
\frac{}{(i, j); (i \geq 1, j \geq 1); \Delta \vdash \text{if } z \text{ then } (\nu c) \cdots \text{else } (\nu c) \cdots \triangleleft i + j - 1} \\
\frac{}{(i, j); (i \geq 1, j \geq 1); \Gamma'', b : \text{ch}_1(\text{Bool}) \vdash b(z) \cdots \triangleleft i + j}
\end{array}$$

And the typing for the other branch of the conditional is similar.

Now, we type the server for the decompose function. We pose:

$$\begin{aligned}
\Gamma' &:= \Gamma_o, l : \text{List}[0, 2i](\mathcal{B}), a_0 : \text{out}_0(\text{List}[0, i](\mathcal{B})), a_1 : \text{out}_0(\text{List}[0, i](\mathcal{B})) \\
\Gamma'' &:= \Gamma', x : \mathcal{B}, q : \text{List}[0, 2i - 1](\mathcal{B}), y : \mathcal{B}, r : \text{List}[0, 2(i - 1)](\mathcal{B}) \\
\Delta &= \Gamma'', b_0 : \text{ch}_0(\text{List}[0, i - 1](\mathcal{B})), b_1 : \text{ch}_0(\text{List}[0, i - 1](\mathcal{B}))
\end{aligned}$$

$$\begin{array}{c}
\frac{}{i; (i \geq 1); \Delta, l_0 : \text{List}[0, i - 1](\mathcal{B}) \vdash \overline{a_0}(x :: l_0) \triangleleft 0} \\
\frac{}{i; (i \geq 1); \Delta \vdash b_0(l_0).\overline{a_0}(x :: l_0) \triangleleft 0} \quad \cdots \\
\frac{}{i; (i \geq 1); \Delta \vdash b_0(l_0).\overline{a_0}(x :: l_0) \mid b_1(l_1).\overline{a_1}(y :: l_1) \triangleleft 0} \\
\frac{}{i; (i \geq 1); \Gamma'', b_0 : \text{ch}_0(\text{List}[0, i - 1](\mathcal{B})), b_1 : \text{ch}_0(\text{List}[0, i - 1](\mathcal{B})) \vdash \overline{\text{decompose}}(r, b_0, b_1) \mid \cdots \triangleleft 0} \\
\frac{}{i; (i \geq 1); \Gamma'' \vdash (\nu b_0)(\nu b_1)(\overline{\text{decompose}}(r, b_0, b_1) \mid \cdots) \triangleleft 0} \\
\frac{}{i; \cdot; \Gamma' \vdash (\overline{a_0}(\square) \mid \overline{a_1}(\square)) \triangleleft 0} \quad \frac{}{i; (2i \geq 1); \Gamma', x : \mathcal{B}, q : \text{List}[0, 2i - 1](\mathcal{B}) \vdash \text{match } q \text{ with } \{\square \mapsto (\overline{a_0}(x :: \square) \mid \overline{a_1}(\square)) \mid y :: r \mapsto \cdots\} \triangleleft 0} \\
\frac{}{i; \cdot; \Gamma' \vdash \text{match } l \text{ with } \{\square \mapsto (\overline{a_0}(\square) \mid \overline{a_1}(\square)) \mid x :: q \mapsto \cdots\} \triangleleft 0} \\
\cdot; \Gamma \vdash !\text{decompose}(l, a_0, a_1) \cdots \triangleleft 0
\end{array}$$

And finally, the typing for the server computing the merge sort. We pose:

$$\begin{aligned}
\Gamma' &:= \Gamma_o, l : \text{List}[0, 2^i](\mathcal{B}), a : \text{out}_{2^{i+1}}(\text{List}[0, 2^i](\mathcal{B})) \\
\Gamma'' &:= \Gamma', x : \mathcal{B}, q : \text{List}[0, 2^i - 1](\mathcal{B}), y : \mathcal{B}, r : \text{List}[0, 2^i - 2](\mathcal{B}) \\
\Delta &= \Gamma'', b_0 : \text{ch}_0(\text{List}[0, 2^{i-1}] (\mathcal{B})), b_1 : \text{ch}_0(\text{List}[0, 2^{i-1}] (\mathcal{B})), \\
c_0 : \text{ch}_{2^i}(\text{List}[0, 2^{i-1}] (\mathcal{B})), c_1 : \text{ch}_{2^i}(\text{List}[0, 2^{i-1}] (\mathcal{B})), d : \text{ch}_{2^{i+1}}(\text{List}[0, 2^i] (\mathcal{B}))
\end{aligned}$$

$$\begin{array}{c}
\text{See below} \\
\frac{}{i; (2^i \geq 2); \Delta \vdash \overline{\text{decompose}}(l, b_0, b_1) \mid \cdots \triangleleft 2^{i+1}} \\
\frac{}{i; (2^i \geq 2); \Gamma'' \vdash (\nu(b_0, b_1, c_0, c_1, d)) \cdots \triangleleft 2^{i+1}} \\
\frac{}{i; \cdot; \Gamma' \vdash \overline{a}(\square) \triangleleft 2^{i+1}} \quad \frac{}{i; (2^i \geq 1); \Gamma', x : \mathcal{B}, q : \text{List}[0, 2^i - 1](\mathcal{B}) \vdash \text{match } q \text{ with } \{\square \mapsto (\overline{a}(x :: \square)) \mid y :: r \mapsto \cdots\} \triangleleft 2^{i+1}} \\
\frac{}{i; \cdot; \Gamma' \vdash \text{match } l \text{ with } \{\square \mapsto \overline{a}(\square) \mid x :: q \mapsto \cdots\} \triangleleft 2^{i+1}} \\
\cdot; \Gamma \vdash !\text{mergesort}(l, a) \cdots \triangleleft 0
\end{array}$$

Where we detail here the different proofs for the 5 processes in parallel.

$$\begin{array}{c}
\frac{i; (2^i \geq 2); \Delta \vdash l : \text{List}[0, 2 * 2^{i-1}](\mathcal{B}) \quad i; (2^i \geq 2); \Delta \vdash b_i : \text{out}_0(\text{List}[0, 2^{i-1}](\mathcal{B}))}{i; (2^i \geq 2); \Delta \vdash \overline{\text{decompose}}\langle l, b_0, b_1 \rangle \triangleleft 0} \\
\frac{}{i; (2^i \geq 2); \Delta \vdash \overline{\text{decompose}}\langle l, b_0, b_1 \rangle \triangleleft 2^{i+1}} \\
\\
\frac{i; (2^i \geq 2); \Delta \vdash l_0 : \text{List}[0, 2^{i-1}](\mathcal{B}) \quad i; (2^i \geq 2); \Delta \vdash c_0 : \text{out}_{2^i}(\text{List}[0, 2^{i-1}](\mathcal{B}))}{i; (2^i \geq 2); \Delta, l_0 : \text{List}[0, 2^{i-1}](\mathcal{B}) \vdash \overline{\text{mergesort}}\langle l_0, c_0 \rangle \triangleleft 2^i} \\
\frac{}{i; (2^i \geq 2); \Delta, l_0 : \text{List}[0, 2^{i-1}](\mathcal{B}) \vdash \overline{\text{mergesort}}\langle l_0, c_0 \rangle \triangleleft 2^{i+1}} \\
\frac{}{i; (2^i \geq 2); \Delta \vdash b_0(l_0).\overline{\text{mergesort}}\langle l_0, c_0 \rangle \triangleleft 2^{i+1}} \\
\\
\frac{i; (2^i \geq 2); \langle \Delta \rangle_{-2^i}, q_0 : \text{List}[0, 2^{i-1}](\mathcal{B}), q_1 : \text{List}[0, 2^{i-1}](\mathcal{B}) \vdash d : \text{ch}_{2^i}(\text{List}[0, 2^i](\mathcal{B}))}{i; (2^i \geq 2); \langle \Delta \rangle_{-2^i}, q_0 : \text{List}[0, 2^{i-1}](\mathcal{B}), q_1 : \text{List}[0, 2^{i-1}](\mathcal{B}) \vdash \overline{\text{merge}}\langle q_0, q_1, d \rangle \triangleleft 2^i} \\
\frac{}{i; (2^i \geq 2); \langle \Delta \rangle_{-2^i}, q_0 : \text{List}[0, 2^{i-1}](\mathcal{B}) \vdash c_1(q_1).\overline{\text{merge}}\langle q_0, q_1, d \rangle \triangleleft 2^i} \\
\frac{}{i; (2^i \geq 2); \Delta \vdash c_0(q_0).c_1(q_1).\overline{\text{merge}}\langle q_0, q_1, d \rangle \triangleleft 2^{i+1}} \\
\\
\frac{i; (2^i \geq 2); \langle \Delta \rangle_{-2^{i+1}}, q_2 : \text{List}[0, 2^i](\mathcal{B}) \vdash a : \text{out}_0(\text{List}[0, 2^i](\mathcal{B}))}{i; (2^i \geq 2); \langle \Delta \rangle_{-2^{i+1}}, q_2 : \text{List}[0, 2^i](\mathcal{B}) \vdash \overline{a}\langle q_2 \rangle \triangleleft 0} \\
\frac{}{i; (2^i \geq 2); \Delta \vdash d(q_2).\overline{a}\langle q_2 \rangle \triangleleft 2^{i+1}}
\end{array}$$

So those servers are well typed under this context. As a consequence, when put in parallel with a call to mergesort with a list of size less than  $N = 2^n$ , we have a bound on the number of comparisons in the computation, and the bound is  $2N$ . In order to explicit the results of Theorem 4, we show how the strategy of Definition 3 works on a call to mergesort.

First, we describe a call to merge with a list of size  $n$  and a list of size  $m$ . In order to simplify the notations, we omit to recall the definition of servers, and we do not write them in the reduction as they are invariant. We consider the case  $n > 0$  and  $m > 0$ , otherwise, there is no tick so there is no time reduction. We also consider  $x_1 \leq y_1$  and the other case is symmetric.

$$\begin{aligned}
\overline{\text{merge}}\langle [x_1; \dots; x_n], [y_1; \dots; y_m], a \rangle &\rightarrow^* (\nu b)(\text{tick}.\overline{\text{compare}}\langle x_1, y_1, b \rangle) \mid b(z).\dots \\
&\Rightarrow (\nu b)(\overline{\text{compare}}\langle x_1, y_1, b \rangle) \mid b(z).\dots \\
&\rightarrow^* (\nu b)(\nu c)(\overline{\text{merge}}\langle [x_2, \dots, x_n], [y_1, \dots, y_m], c \rangle \mid c(l_2).\overline{a}\langle x_1 :: l_2 \rangle)
\end{aligned}$$

Then, we can show by induction that the number of step reduction is less than  $n + m$  and that a call to merge produces at the end an output on the channel (and some name variables that we omit for simplicity). And then, we have:

$$(\nu b)(\nu c)(\overline{c}\langle [z_1; \dots; z_{n+m-1}] \rangle \mid c(l_2).\overline{a}\langle x_1 :: l_2 \rangle) \rightarrow^* (\nu b)(\nu c)(\overline{a}\langle x_1 :: [z_1; \dots; z_{n+m-1}] \rangle)$$

So we have indeed less than  $n + m$  time reductions. In a call to decompose, no time reduction occurs, so the reduction has indeed complexity 0. For the example, we show a call to mergesort on a list of size 4 and show that we have a bound of 8 time reductions. The general behaviour can be deduced from this example.

$$\begin{aligned}
& \overline{\text{mergesort}}\langle [4; 6; 7; 2], a \rangle \rightarrow^* (\nu(b_0, b_1, c_0, c_1, d))(\overline{\text{decompose}}\langle [4; 6; 7; 2], b_0, b_1 \rangle \mid \dots) \\
& \rightarrow^* (\nu(b_0, b_1, c_0, c_1, d))(\overline{\text{mergesort}}\langle [4; 7], c_0 \rangle \mid \overline{\text{mergesort}}\langle [6; 2], c_1 \rangle \mid c_0(q_0).c_1(q_1).\dots \mid d(q_2).\dots) \\
& \rightarrow^* (\nu(\dots))(\overline{\text{mergesort}}\langle [4], c'_0 \rangle \mid \overline{\text{mergesort}}\langle [7], c'_1 \rangle \mid c'_0(q_0).c'_1(q_1).\dots \mid d'(q_2).\dots) \\
& \mid \overline{\text{mergesort}}\langle [6], c''_0 \rangle \mid \overline{\text{mergesort}}\langle [2], c''_1 \rangle \mid c''_0(q_0).c''_1(q_1).\dots \mid d''(q_2).\dots \mid c_0(q_0).c_1(q_1).\dots \mid d(q_2).\dots) \\
& \rightarrow^* (\nu(\dots))(\overline{c}_0\langle [4] \rangle \mid \overline{c}_1\langle [7] \rangle \mid c'_0(q_0).c'_1(q_1).\dots \mid d'(q_2).\dots) \\
& \mid \overline{c}''_0\langle [6] \rangle \mid \overline{c}''_1\langle [2] \rangle \mid c''_0(q_0).c''_1(q_1).\dots \mid d''(q_2).\dots \mid c_0(q_0).c_1(q_1).\dots \mid d(q_2).\dots) \\
& \rightarrow^* (\nu(\dots))(\overline{\text{merge}}\langle [4], [7], d' \rangle \mid d'(q_2).\dots \mid \overline{\text{merge}}\langle [6], [2], d'' \rangle \mid d''(q_2).\dots \mid c_0(q_0).c_1(q_1).\dots \mid d(q_2).\dots) \\
& \rightarrow^* (\nu(\dots))(\text{tick}.\overline{\text{compare}}\langle 4, 7, b \rangle \mid b(z).\dots \mid d'(q_2).\dots \mid \\
& \text{tick}.\overline{\text{compare}}\langle 6, 2, b' \rangle \mid b'(z).\dots \mid d''(q_2).\dots \mid c_0(q_0).c_1(q_1).\dots \mid d(q_2).\dots)
\end{aligned}$$

And this process is in normal form for  $\rightarrow$ . Thus, we can do the time reduction.

$$\begin{aligned}
& \Rightarrow (\nu(\dots))(\overline{\text{compare}}\langle 4, 7, b \rangle \mid b(z).\dots \mid d'(q_2).\dots \mid \\
& \overline{\text{compare}}\langle 6, 2, b' \rangle \mid b'(z).\dots \mid d''(q_2).\dots \mid c_0(q_0).c_1(q_1).\dots \mid d(q_2).\dots) \\
& \rightarrow^* (\nu(\dots))(\overline{d}\langle [4; 7] \rangle \mid d'(q_2).\dots \mid \overline{d}''\langle [2; 6] \rangle \mid d''(q_2).\dots \mid c_0(q_0).c_1(q_1).\dots \mid d(q_2).\dots) \\
& \rightarrow^* (\nu(\dots))(\overline{c}_0\langle [4; 7] \rangle \mid \overline{c}_1\langle [2; 6] \rangle \mid c_0(q_0).c_1(q_1).\dots \mid d(q_2).\dots) \\
& \rightarrow^* (\nu(\dots))(\overline{\text{merge}}\langle [4; 7], [2; 6], d \rangle \mid d(q_2).\overline{a}\langle q_2 \rangle)
\end{aligned}$$

And, with what we saw before, we can do the merging in at most 4 time reductions, and finish the computation.

If we want a more generic notion of complexity for programs, we believe it is best to consider the number of communications on channels. A good way to count this is to add a tick after each input (we could also add a tick before each input, or before each output, however in this case, stuck programs would have a complexity 1 even if they do not communicate, that is why we believe it is better to put them after the input). Without detailing the typing, we give the complexity for mergesort in this case. We suppose that the complexity of compare is  $K_c$ .

For the merge function, if we call  $f(i, j)$  the complexity of a call to merge on input of sizes between 0 and  $i$  and 0 and  $j$ , we obtain the following restrictions in the typing:

$$f(i, j) \geq 1 \quad \forall i, j \geq 1, f(i, j) \geq f(i-1, j) + K_c + 3 \quad \forall i, j \geq 1, f(i, j) \geq f(i, j-1) + K_c + 3$$

Indeed, we always start by a tick, so the complexity for any call is more than 1. Then, in the computation, when the lists are not empty, we have a total of 3 input, a call to compare and a call to merge where the size of one of the list decrease by one. So, we could for example take

$$f(i, j) = (3 + K_c)(i + j) + 1$$

Now, for the decompose function, if we call  $f(i)$  the complexity for an input list of size smaller than  $2i$ , we obtain the following restrictions:

$$f(i) \geq 1 \quad \forall i \geq 1, f(i) \geq 2 + f(i-1)$$

Thus, we obtain the complexity

$$f(i) = 1 + 2i$$

Finally, for the merge sort, we obtain the following restrictions, if we call  $f(i)$  the complexity on an input list of size smaller than  $2^i$ .

$$f(i) \geq 1 \quad \forall i \geq 1, f(i) \geq 1 + 1 + 2^i + 1 + f(i-1) + 2 + (3 + K_c)2^i + 1 + 1$$

|   |   |   |  |
|---|---|---|--|
| $\frac{P \xrightarrow{\text{tick}} P'}{P \mid Q \xrightarrow{\text{tick}} P' \mid Q}$ | $\frac{Q \xrightarrow{\text{tick}} Q'}{P \mid Q \xrightarrow{\text{tick}} P \mid Q'}$ | $\frac{P \xrightarrow{\text{tick}} P'}{(\nu a)P \xrightarrow{\text{tick}} (\nu a)P'}$ | $\frac{}{\text{tick}.P \xrightarrow{\text{tick}} P}$ |
|---|---|---|--|

Figure 10: Tick Reduction Rules

Indeed, we start with a tick (+1), then a call to decompose ( $1+2^i$ ), then we get back the results (+1) and call two mergesort ( $f(i-1)$ ) in parallel, then we get back the results (+2) and call merge ( $(3+K_c)2^i+1$ ), and finally we get back the result (+1) and send it to the output channel. So, finally, we obtain

$$f(i) \geq 1 \quad \forall i \geq 1, f(i) \geq 7 + f(i-1) + (4+K_c)2^i$$

, thus

$$f(i) = 1 + 7i + (4+K_c)(2^{i+1} - 2)$$

Remark that if we only look at the coefficient for  $K_c$ , we get back the complexity for the number of comparison. Anyway, mergesort is indeed linear under maximal parallelism with this result.

## 6 Work of a Process

We now want to obtain the total complexity of a process, that is to say the total number of tick without parallelism. We will see that this notion of complexity is far easier to obtain. First, let us define the new time reduction we are interested in  $\xrightarrow{\text{tick}}$ . This is defined in Figure 10.

And then, from any process  $P$ , a reduction to  $Q$  is just a sequence of one-step reductions with  $\rightarrow$  or  $\xrightarrow{\text{tick}}$ , and the complexity of this reduction is the number of  $\xrightarrow{\text{tick}}$ . Contrary to the tick-last strategy, we do not add any restrictions on this semantic. We will now again design a type system to obtain a bound on the complexity of all possible reductions from  $P$ . We will see that this type system is more permissive than the previous one, and is a simplification of the previous one.

**Definition 13.** *The set of types and base types are given by the following grammar.*

$$\begin{aligned} \mathcal{B} &:= \text{Nat}[I, J] \mid \text{List}[I, J](\mathcal{B}) \mid \text{Bool} \\ \mathcal{T} &:= \mathcal{B} \mid \text{ch}(\tilde{T}) \mid \text{in}(\tilde{T}) \mid \text{out}(\tilde{T}) \mid \forall i.\text{serv}^K(\tilde{T}) \mid \forall i.\text{iserv}^K(\tilde{T}) \mid \forall i.\text{oserv}^K(\tilde{T}) \end{aligned}$$

Note that there are no time indication in those types. Then, the subtyping system is given in Figure 11. It is very close to the previous one.

And then, the typing for expressions is the same as before, and for processes we take the rules of Figure 12.

With this type system, we obtain as before some lemmas such as weakening (Lemma 13), strengthening (Lemma 14), index substitution (Lemma 15) and finally substitution (Lemma 17). With those, we can show with a simpler proof than before the non-quantitative subject reduction (Theorem 2). Then, we can show the following theorem:

**Theorem 5 (Work Complexity).** *If  $P \xrightarrow{\text{tick}} Q$  and  $\phi; \Phi; \Gamma \vdash P \triangleleft K$  then we have  $\phi; \Phi; \Gamma \vdash Q \triangleleft K'$  with  $\phi; \Phi \vDash K' + 1 \leq K$ .*

*Proof.* By induction on  $P \xrightarrow{\text{tick}} Q$ . All the cases are direct, since the rule for parallel composition is the sum of complexity and the rule for  $\nu$  does not change the complexity. Finally, the rule for tick gives directly this propriety.  $\square$

So, as a consequence we obtain quasi immediately that  $K$  is indeed a bound on the complexity of  $P$  if we have  $\phi; \Phi; \Gamma \vdash P \triangleleft K$ . As we can see, this complexity is far more easier to obtain than the span as the parallelism is not really taken in account. That is why we think the span is a good notion of complexity if we want to focus on parallelism.

|  |   |   |
|--|---|---|
| $\frac{\phi; \Phi \vDash I' \leq I \quad \phi; \Phi \vDash J \leq J'}{\phi; \Phi \vdash \text{Nat}[I, J] \sqsubseteq \text{Nat}[I', J']}$  | $\frac{\phi; \Phi \vDash I' \leq I \quad \phi; \Phi \vDash J \leq J' \quad \phi; \Phi \vdash \mathcal{B} \sqsubseteq \mathcal{B}'}{\phi; \Phi \vdash \text{List}[I, J](\mathcal{B}) \sqsubseteq \text{List}[I', J'](\mathcal{B}')}$ |   |
| $\frac{}{\phi; \Phi \vdash \text{Bool} \sqsubseteq \text{Bool}}$   | $\frac{\phi; \Phi \vdash \tilde{T} \sqsubseteq \tilde{U} \quad \phi; \Phi \vdash \tilde{U} \sqsubseteq \tilde{T}}{\phi; \Phi \vdash \text{ch}(\tilde{T}) \sqsubseteq \text{ch}(\tilde{U})}$   | $\frac{}{\phi; \Phi \vdash \text{ch}(\tilde{T}) \sqsubseteq \text{in}(\tilde{T})}$  |
| $\frac{}{\phi; \Phi \vdash \text{ch}(\tilde{T}) \sqsubseteq \text{out}(\tilde{T})}$  | $\frac{\phi; \Phi \vdash \tilde{T} \sqsubseteq \tilde{U}}{\phi; \Phi \vdash \text{in}(\tilde{T}) \sqsubseteq \text{in}(\tilde{U})}$   | $\frac{\phi; \Phi \vdash \tilde{U} \sqsubseteq \tilde{T}}{\phi; \Phi \vdash \text{out}(\tilde{T}) \sqsubseteq \text{out}(\tilde{U})}$ |
| $\frac{(\phi, \tilde{i}); \Phi \vdash \tilde{T} \sqsubseteq \tilde{U} \quad (\phi, \tilde{i}); \Phi \vdash \tilde{U} \sqsubseteq \tilde{T} \quad (\phi, \tilde{i}); \Phi \vDash K = K'}{\phi; \Phi \vdash \forall \tilde{i}. \text{serv}^K(\tilde{T}) \sqsubseteq \forall \tilde{i}. \text{serv}^{K'}(\tilde{U})}$ |   |   |
| $\frac{}{\phi; \Phi \vdash \forall \tilde{i}. \text{serv}^K(\tilde{T}) \sqsubseteq \forall \tilde{i}. \text{iserv}^K(\tilde{T})} \quad \frac{}{\phi; \Phi \vdash \forall \tilde{i}. \text{serv}^K(\tilde{T}) \sqsubseteq \forall \tilde{i}. \text{oserv}^K(\tilde{T})}$  |   |   |
| $\frac{(\phi, \tilde{i}); \Phi \vdash \tilde{T} \sqsubseteq \tilde{U} \quad (\phi, \tilde{i}); \Phi \vDash K' \leq K}{\phi; \Phi \vdash \forall \tilde{i}. \text{iserv}^K(\tilde{T}) \sqsubseteq \forall \tilde{i}. \text{iserv}^{K'}(\tilde{U})}$   |   |   |
| $\frac{(\phi, \tilde{i}); \Phi \vdash \tilde{U} \sqsubseteq \tilde{T} \quad (\phi, \tilde{i}); \Phi \vDash K \leq K'}{\phi; \Phi \vdash \forall \tilde{i}. \text{oserv}^K(\tilde{T}) \sqsubseteq \forall \tilde{i}. \text{oserv}^{K'}(\tilde{U})}$   | $\frac{\phi; \Phi \vdash T \sqsubseteq T' \quad \phi; \Phi \vdash T' \sqsubseteq T''}{\phi; \Phi \vdash T \sqsubseteq T''}$   |   |

Figure 11: Subtyping Rules for Sized Types

|   |  |  |
|---|--|--|
| $\frac{}{\phi; \Phi; \Gamma \vdash 0 \triangleleft 0}$  | $\frac{\phi; \Phi; \Gamma \vdash P \triangleleft K \quad \phi; \Phi; \Gamma \vdash Q \triangleleft K'}{\phi; \Phi; \Gamma \vdash P \mid Q \triangleleft K + K'}$                 |  |
| $\frac{\phi; \Phi; \Gamma \vdash a : \forall \tilde{i}. \text{iserv}^K(\tilde{T}) \quad (\phi, \tilde{i}); \Phi; \Gamma, \tilde{v} : \tilde{T} \vdash P \triangleleft K}{\phi; \Phi; \Gamma \vdash !a(\tilde{v}).P \triangleleft 0}$  |  |  |
| $\frac{\phi; \Phi; \Gamma \vdash a : \text{in}(\tilde{T}) \quad \phi; \Phi; \Gamma, \tilde{v} : \tilde{T} \vdash P \triangleleft K}{\phi; \Phi; \Gamma \vdash a(\tilde{v}).P \triangleleft K}$  | $\frac{\phi; \Phi; \Gamma \vdash a : \text{out}(\tilde{T}) \quad \phi; \Phi; \Gamma \vdash \tilde{e} : \tilde{T}}{\phi; \Phi; \Gamma \vdash \bar{a}(\tilde{e}) \triangleleft 0}$ |  |
| $\frac{\phi; \Phi; \Gamma \vdash a : \forall \tilde{i}. \text{oserv}^K(\tilde{T}) \quad \phi; \Phi; \Gamma \vdash \tilde{e} : \tilde{T}\{\tilde{J}/\tilde{i}\}}{\phi; \Phi; \Gamma \vdash \bar{a}(\tilde{e}) \triangleleft K\{\tilde{J}/\tilde{i}\}}$   | $\frac{\phi; \Phi; \Gamma, a : T \vdash P \triangleleft K}{\phi; \Phi; \Gamma \vdash (\nu a)P \triangleleft K}$  |  |
| $\frac{\phi; \Phi; \Gamma \vdash e : \text{Nat}[I, J] \quad \phi; (\Phi, I \leq 0); \Gamma \vdash P \triangleleft K \quad \phi; (\Phi, J \geq 1); \Gamma, x : \text{Nat}[I-1, J-1] \vdash Q \triangleleft K}{\phi; \Phi; \Gamma \vdash \text{match } e \text{ with } \{0 \mapsto P \mid s(x) \mapsto Q\} \triangleleft K}$  |  |  |
| $\frac{\phi; \Phi; \Gamma \vdash e : \text{List}[I, J](\mathcal{B}) \quad \phi; (\Phi, I \leq 0); \Gamma \vdash P \triangleleft K \quad \phi; (\Phi, J \geq 1); \Gamma, x : \mathcal{B}, y : \text{List}[I-1, J-1](\mathcal{B}) \vdash Q \triangleleft K}{\phi; \Phi; \Gamma \vdash \text{match } e \text{ with } \{\square \mapsto P \mid x :: y \mapsto Q\} \triangleleft K}$ |  |  |
| $\frac{\phi; \Phi; \Gamma \vdash e : \text{Bool} \quad \phi; \Phi; \Gamma \vdash P \triangleleft K \quad \phi; \Phi; \Gamma \vdash Q \triangleleft K}{\phi; \Phi; \Gamma \vdash \text{if } e \text{ then } P \text{ else } Q \triangleleft K}$  | $\frac{\phi; \Phi; \Gamma \vdash P \triangleleft K}{\phi; \Phi; \Gamma \vdash \text{tick}.P \triangleleft K + 1}$  |  |
| $\frac{\phi; \Phi; \Delta \vdash P \triangleleft K \quad \phi; \Phi \vdash \Gamma \sqsubseteq \Delta \quad \phi; \Phi \vDash K \leq K'}{\phi; \Phi; \Gamma \vdash P \triangleleft K'}$  |  |  |

Figure 12: Typing Rules for Processes

```

!merge( $l_0, l_1, a$ ). match  $l_0$  with
| []  $\mapsto \bar{a}\langle l_1 \rangle$ 
|  $x :: q \mapsto$  match  $l_1$  with
| []  $\mapsto \bar{a}\langle l_0 \rangle$ 
|  $y :: r \mapsto (\nu b)(\nu c_1)(\nu c_2)(\text{tick}.\overline{\text{compare}}\langle x, y, b \rangle \mid \overline{\text{merge}}\langle q, l_1, c_1 \rangle \mid \overline{\text{merge}}\langle l_0, r, c_2 \rangle \mid$ 
 $b\langle z \rangle$ . if  $z$  then  $c_1\langle l_2 \rangle.\bar{a}\langle x :: l_2 \rangle$  else  $c_2\langle l_2 \rangle.\bar{a}\langle y :: l_2 \rangle$ 
)

```

Figure 13: Alternative Merge

## 7 Other Results

### 7.1 Work for Mergesort in the Number of Comparisons

Without detailing the typing derivation, we give the work for mergesort. The detailed derivation looks like the one for the span, and so we only give the equations that the complexity must satisfy.

For merge, if we call  $f(i, j)$  the complexity of a call to merge on a list of size smaller than  $i$  and a list of size smaller than  $j$ , we have:

$$\forall i, j \geq 1, f(i, j) \geq 1 + f(i-1, j) \text{ and } f(i, j) \geq 1 + f(i, j-1)$$

So we can take the complexity  $f(i, j) = i + j$ .

Then, the decompose has a complexity 0 since it does not involve any comparison. Finally, if we denote  $f(i)$  the complexity of a call to mergesort on a list of size smaller than  $2^i$ , we have:

$$\forall i \geq 1, f(i) \geq f(i-1) + f(i-1) + 2^i$$

So, we can take the complexity  $f(i) = i * 2^i$ , and we obtain as expected a complexity in  $n \log(n)$ .

### 7.2 Work for Mergesort for the Number of Communication

Then, as before, we could also consider a tick after each input, in order to take in account the communication complexity. As before, let  $K_c$  be the complexity of a call to compare, we then obtain the following complexities:

For merge, we have:

$$f(i, j) \geq 1 \quad \forall i, j \geq 1, f(i, j) \geq 1 + K_c + 1 + f(i-1, j) + 1 \text{ and } f(i, j) \geq 1 + K_c + 1 + f(i, j-1) + 1$$

So, we obtain  $f(i, j) = (3 + K_c)(i + j) + 1$ .

For decompose, we have, on a list of size  $2i$ :

$$f(i) \geq 1 \quad \forall i \geq 1, f(i) \geq 1 + f(i-1) + 2$$

So, we obtain  $f(i) = 3i + 1$ .

Finally, for merge sort we obtain, on a list of size  $2^i$ :

$$f(i) \geq 1 + 3 * 2^{i-1} + 1 + 1 + f(i-1) + 1 + f(i-1) + 2 + (3 + K_c)2^i + 1 + 1$$

$$f(i) \geq 8 + (4.5 + K_c)2^i + 2f(i-1)$$

So we can take  $f(i) = 8(2^{i+1} - 1) + (4.5 + K_c)i2^i$ .

### 7.3 Another Way to Merge

An alternative version of merge is given in Figure 13. The idea of this alternative version compared to Figure 9 is to compute both results of the conditional before even receiving the results of the conditional



- [6] Paolo Di Giamberardino and Ugo Dal Lago. On session types and polynomial time. *Mathematical Structures in Computer Science*, -1, 2015.
- [7] Jan Hoffmann, Klaus Aehlig, and Martin Hofmann. Resource aware ML. In *Computer Aided Verification - 24th International Conference, CAV 2012, Berkeley, CA, USA, July 7-13, 2012 Proceedings*, volume 7358 of *Lecture Notes in Computer Science*, pages 781–786. Springer, 2012.
- [8] John Hughes, Lars Pareto, and Amr Sabry. Proving the correctness of reactive systems using sized types. In *Proceedings of the 23rd ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 410–423. ACM, 1996.
- [9] Naoki Kobayashi. A type system for lock-free processes. *Information and Computation*, 177(2):122 – 159, 2002.
- [10] Naoki Kobayashi, Benjamin C. Pierce, and David N. Turner. Linearity and the pi-calculus. *ACM Trans. Program. Lang. Syst.*, 21(5):914–947, sep 1999.
- [11] Ugo Dal Lago, Simone Martini, and Davide Sangiorgi. Light logics and higher-order processes. *Mathematical Structures in Computer Science*, 26(6):969–992, 2016.
- [12] Antoine Madet and Roberto M. Amadio. An elementary affine  $\lambda$ -calculus with multithreading and side effects. In *Typed Lambda Calculi and Applications - 10th International Conference, TLCA 2011, Novi Sad, Serbia, June 1-3, 2011. Proceedings*, volume 6690 of *Lecture Notes in Computer Science*, pages 138–152. Springer, 2011.
- [13] Davide Sangiorgi and David Walker. *The pi-calculus: a Theory of Mobile Processes*. Cambridge university press, 2003.