

# Encodability and Separation for a Reflective Higher-Order Calculus\*

Stian Lybech

Reykjavík University  
Reykjavík, Iceland  
stian21@ru.is

The  $\rho$ -calculus (Reflective Higher-Order Calculus) of Meredith and Radestock is a  $\pi$ -calculus-like language with some unusual features, notably, structured names, runtime generation of free names, and the lack of an operator for scoping visibility of names. These features pose some interesting difficulties for proofs of encodability and separation results. We describe two errors in a previously published attempt to encode the  $\pi$ -calculus in the  $\rho$ -calculus by Meredith and Radestock. Then we give a new encoding and prove its correctness, using a set of encodability criteria close to those proposed by Gorla, and discuss the adaptations necessary to work with a calculus with runtime generation of structured names. Lastly we prove a separation result, showing that the  $\rho$ -calculus cannot be encoded in the  $\pi$ -calculus.

## 1 Introduction

Process calculi are formalisms for modelling and reasoning about concurrent and distributed computations; a prominent example is the  $\pi$ -calculus of Milner, Parrow and Walker [13, 12]. These languages commonly begin by assuming a *countably infinite set of atomic names*  $\mathcal{N}$ , ranged over by  $x, y, z$ . This is not an unreasonable assumption for most purposes, but it does leave open the question of how this set of names should actually be interpreted, e.g. if we were to create an implementation of the  $\pi$ -calculus or one of its variants [20, 16, 5].

A similar issue arises with the scoping operator  $(\nu x)P$ , which is used to declare a new name  $x$  with visibility limited to  $P$ . Here the question becomes how we should choose this new name  $x$ , such that it is actually ensured to be unique. For a process modelling a program running on a single computer, this can easily be solved, e.g. with a counter; but if the process models a *distributed* system, with programs running on distinct computers, the solution is less obvious. These issues are not directly handled in the  $\pi$ -calculus model, but only become apparent when we consider a more practical implementation of the set of names.

A radically different approach is taken in the Reflective Higher-Order (RHO or  $\rho$ ) calculus proposed by Meredith and Radestock in [11]. These authors instead begin by positing that the set of names is built by a syntax, similar to the syntax for processes, and thus generated from a *finite* set of elements. One could imagine different possibilities for this syntax, but Meredith and Radestock here make the unusual choice of letting names be ‘quoted’ processes, written  $\ulcorner P \urcorner$ . Thus, if  $P$  is a process, then  $\ulcorner P \urcorner$  is a name. This creates a mutually recursive definition, since processes also contain names. The full syntax of the  $\rho$ -calculus is then

$$\begin{aligned} P \in \mathcal{P}_\rho &::= \mathbf{0} \mid P_1 \mid P_2 \mid x \langle P \rangle \mid x(y).P \mid \ulcorner x \urcorner \\ x, y \in \ulcorner \mathcal{P}_\rho \urcorner &::= \ulcorner P \urcorner \end{aligned}$$

---

\*This work was supported by the Icelandic Research Fund Grant No. 218202-05(1-3).

Three of the constructs are as in the  $\pi$ -calculus: The *nil* process,  $\mathbf{0}$ , is the inactive process; The *parallel* construct,  $P_1 \mid P_2$ , is the parallel composition of processes  $P_1$  and  $P_2$ ; and the *input* construct,  $x(y).P$ , is a blocking operation, awaiting a communication on the channel  $x$  of some name, which, upon reception, will be bound to  $y$  in the continuation  $P$ .

The two remaining constructs are particular to the  $\rho$ -calculus: The *lift* construct  $x \langle P \rangle$  quotes the process  $P$ , thereby creating the name  $\ulcorner P \urcorner$ , and outputs it on  $x$ ; thus name generation is handled explicitly in the  $\rho$ -calculus, rather than implicitly by a  $\pi$ -calculus style  $\nu$ -operator. This is the second peculiarity of this calculus, since the newly generated name will be *free* in the continuation of the corresponding input, and therefore also *observable* if substituted for the subject of an input or lift. As we shall later see, this feature is crucial for showing a separation result w.r.t. the  $\pi$ -calculus.

Lastly, the *drop* construct  $\lrcorner x \lrcorner$  removes the quotes of the name to run the process within them, thereby enabling higher-order behaviour (i.e. process mobility). This construct is thus similar to a process variable  $X$  in e.g.  $\text{HO}\pi$  [17, 18], and is also the reason for the ‘reflective’ epithet in the name of this calculus. It derives from Smith [19], who defined reflection as the ability of a program to turn code into data, compute with it, modify it, and turn it back into running code, which in the  $\rho$ -calculus is captured by the combination of the lift and drop constructs, and the duality of names and processes.

Although superficially quite similar to the  $\pi$ -calculus, these features suggest that the  $\rho$ -calculus is actually rather different. As argued above, the use of structured terms as names, and explicit name generation, seem more realistic from an implementation perspective, as it places the problems of choosing the next name, and of ensuring freshness, within the language itself, rather than simply assuming that these features just work behind the scenes. However, providing a *solution* to these problems is not trivial, as we shall see below. For example, in [11] Meredith and Radestock also propose an encoding of the asynchronous, choice-free fragment of the  $\pi$ -calculus into the  $\rho$ -calculus, reviewed in section 3, but as we shall show in section 4, this encoding contains two fatal errors, invalidating their correctness result.

In what follows, we shall instead propose a different encoding of the  $\pi$ -calculus into the  $\rho$ -calculus and formally prove its correctness w.r.t. a number of encodability criteria closely related to those proposed by Gorla in [8], but with some adaptations necessitated by the aforementioned peculiar features of the  $\rho$ -calculus (Propositions 1-5). Using the same criteria we then derive a separation result, showing that the converse of this statement does not hold: there cannot be an encoding of the  $\rho$ -calculus into the  $\pi$ -calculus satisfying the same criteria (Theorem 1).<sup>1</sup> This result is quite surprising, and it suggests that we cannot always just reduce higher-order behaviour to the first-order paradigm, as Sangiorgi was able to do with  $\text{HO}\pi$  in [18]. This is because higher-order behaviour in the  $\rho$ -calculus is not just an extension on top of an already computationally complete language, as it is the case with  $\text{HO}\pi$  which extends the ‘first-order’  $\pi$ -calculus, but rather appears as a special case of the more general phenomenon of reflection, where processes (code) are communicated without modification.

## 2 The Reflective Higher-Order Calculus

We begin by presenting the  $\rho$ -calculus following Meredith and Radestock in [11]. As we have already seen the syntax above, we shall here focus on the semantics, which we shall give in terms of a reduction system. Firstly, we shall need a notion of *structural congruence* on processes, written  $\equiv$ . We shall postpone its precise definition slightly, but the intuition is that  $P_1 \equiv P_2$  denotes that  $P_1$  and  $P_2$  are the same process, up to some insignificant structural change, such as reordering of components in parallel composition or a change of bound names ( $\alpha$ -conversion).

<sup>1</sup>Full proofs of most results are available in a technical report [10].

Now, since names are quoted processes, this notion of structural congruence is extended to the set of names: the *name equivalence* relation, written  $\equiv_{\mathcal{N}}$ , is defined as the least equivalence on names closed under the following rules:

$$[\text{N-STRUCT}] \frac{P_1 \equiv P_2}{\ulcorner P_1 \urcorner \equiv_{\mathcal{N}} \ulcorner P_2 \urcorner} \quad [\text{N-DROP}] \frac{x_1 \equiv_{\mathcal{N}} x_2}{\ulcorner x_1 \urcorner \equiv_{\mathcal{N}} x_2}$$

The point of [N-STRUCT] is that if the processes within quotes have the same structure (up to structural congruence), then the quoted processes should also represent the same name. Furthermore, by [N-DROP], we allow nested levels of quotes and drops to ‘cancel out.’

Next, we shall need the notions of free and bound names,  $\text{fn}(P)$  and  $\text{bn}(P)$ , which are defined in the usual (syntactic) way, with input being the only formal binder in the language. Thus  $\text{bn}(x(y).P) = \{y\} \cup \text{bn}(P)$ , and all other names are free. We write  $\text{n}(P) \triangleq \text{fn}(P) \cup \text{bn}(P)$  for all the names in  $P$ , and we also write  $x\#P$  to mean that  $x$  is *fresh* for  $P$ . However, with *structured* names, it is no longer enough that  $x \notin \text{n}(P)$ ;  $x$  must also not be *name equivalent* to any name in  $P$ . Thus we say  $x\#P \triangleq \forall n \in \text{n}(P) . x \not\equiv_{\mathcal{N}} n$ . Lastly, we write  $P\{x/y\}$  for the safe substitution of  $x$  for  $y$  within  $P$ . However, given our considerations about  $\equiv_{\mathcal{N}}$  above,  $P\{x/y\}$  will not only replace  $y$ , but also any name that is *name equivalent* to  $y$ . Note also, in particular, that substitution does *not* recur into processes under quotes. Thus  $\ulcorner P \urcorner \{x/y\} = \ulcorner P \urcorner$  for all names  $y$  where  $y \not\equiv_{\mathcal{N}} \ulcorner P \urcorner$ , and  $\ulcorner P \urcorner \{x/y\} = x$  otherwise.

We shall now return to the definition of structural congruence: it is defined as the usual least congruence on processes, containing  $\alpha$ -equivalence and the abelian monoid rules for parallel composition with  $\mathbf{0}$  as the unit element. However, with structured terms as names, the congruence rules take on a slightly unusual form, since we now also need to compare names. For example, to conclude  $x_1(y_1).P_1 \equiv x_2(y_2).P_2$  we would need the following rule in structural congruence:

$$[\text{S-IN}] \frac{x_1 \equiv_{\mathcal{N}} x_2 \quad P_1\{z/y_1\} \equiv P_2\{z/y_2\}}{x_1(y_1).P_1 \equiv x_2(y_2).P_2} \quad (z\#P_1, P_2)$$

This yields another mutual recursion between structural congruence and name equivalence.

With these concepts in place, we can at last give the reduction rules for our semantics as follows:

$$[\rho\text{-PAR}] \frac{P_1 \rightarrow P'_1}{P_1 \mid P_2 \rightarrow P'_1 \mid P_2} \quad [\rho\text{-STRUCT}] \frac{P_1 \equiv P'_1 \quad P'_1 \rightarrow P'_2 \quad P'_2 \equiv P_2}{P_1 \rightarrow P_2}$$

$$[\rho\text{-COM}] \frac{x_1 \equiv_{\mathcal{N}} x_2}{x_1(y).P_1 \mid x_2 \langle P_2 \rangle \rightarrow P_1 \{ \ulcorner P_2 \urcorner / y \}}$$

The  $[\rho\text{-PAR}]$  and  $[\rho\text{-STRUCT}]$  rules are standard (as in e.g. the  $\pi$ -calculus); the former lets us conclude a reduction of one component in a parallel composition, whilst the latter allows us to rewrite the process, using structural congruence  $\equiv$ , such that its form can match the conclusion of one of the other rules.

The  $[\rho\text{-COM}]$  rule is also *almost* standard: The process  $P_2$  is quoted and sent out over  $x_2$ , and the matching input receives it as the name  $\ulcorner P_2 \urcorner$  and substitutes it for  $y$  in the continuation  $P_1$ . However, since names in the  $\rho$ -calculus have structure, we must be able to explicitly conclude the equivalence  $x_1 \equiv_{\mathcal{N}} x_2$  between the two subjects in a communication. This is thus different from calculi with atomic names where exact syntactic equality is (usually implicitly) required between subjects.

One last detail concerns substitution: In structural congruence, including  $\alpha$ -equivalence,  $P\{x/y\}$  is defined as the usual capture-avoiding substitution of names for names. However, the substitution used in the *semantics* is slightly different, as it is also used to handle the  $\ulcorner x \urcorner$  construct, which was not given a reduction rule above. The semantic substitution also contains the clause  $\ulcorner x \urcorner \{ \ulcorner P \urcorner / y \} = P$  if  $x \equiv_{\mathcal{N}} y$ , thus replacing the *process*  $\ulcorner x \urcorner$  with  $P$ ; and  $\ulcorner x \urcorner \{ \ulcorner P \urcorner / y \} = \ulcorner x \urcorner$  if  $x \not\equiv_{\mathcal{N}} y$ . This is the only way in which a  $\ulcorner x \urcorner$  is ever executed, and it implies that the drop of a *free* name is a deadlock, as it can never be touched by a substitution at runtime.

### 3 The encoding of Meredith and Radestock

In [11], Meredith and Radestock proposed an encoding of the asynchronous, choice-free  $\pi$ -calculus, taking full abstraction w.r.t. weak, barbed bisimilarity as their correctness criterion. Unfortunately, that encoding is *not* correct, as we shall now show. The counter-examples are instructive, as they highlight some of the difficulties inherent in working with a calculus without the assumption of an infinite set of atomic names and explicit scoping operators.

First, we recall the syntax and semantics of the asynchronous choice-free  $\pi$ -calculus, as given e.g. in [14]. Note that some of the constructs and concepts are similar to those found in the  $\rho$ -calculus. We shall therefore reuse some of the symbols and rely on context to distinguish whether a  $\pi$ -calculus or  $\rho$ -calculus construct is meant. The syntax is:

$$P \in \mathcal{P}_\pi ::= \mathbf{0} \mid P_1 \mid P_2 \mid x(y).P \mid \bar{x}\langle z \rangle \mid (vx)P \mid !P$$

The semantics is given in terms of a reduction system with the rules

$$[\pi\text{-COM}] \frac{}{x(y).P \mid \bar{x}\langle z \rangle \rightarrow P\{z/y\}} \quad [\pi\text{-RES}] \frac{P \rightarrow P'}{(vx)P \rightarrow (vx)P'}$$

and with rules for parallel composition and structural congruence similar to those in the  $\rho$ -calculus (rules  $[\rho\text{-PAR}]$  and  $[\rho\text{-STRUCT}]$  above). Structural congruence  $\equiv$  over  $\mathcal{P}_\pi$  contains the same rules as in the  $\rho$ -calculus, but with syntactic equality replacing name equivalence, and also the following rules for scoping and replication:

$$\begin{aligned} (vx)\mathbf{0} &\equiv \mathbf{0} & !P &\equiv P \mid !P \\ (vx)(vy)P &\equiv (vy)(vx)P & (vx)P_1 \mid P_2 &\equiv (vx)(P_1 \mid P_2) \text{ if } x \notin \text{fn}(P_2) \end{aligned}$$

Now for the encoding, assume a function  $\varphi : \mathcal{N} \rightarrow \ulcorner \mathcal{P}_\rho \urcorner$  from  $\pi$ -calculus atomic names to  $\rho$ -calculus names. Since the set of  $\pi$ -calculus names is countably infinite, it can for example be mapped to the set of natural numbers. The function  $\varphi$  could then be regarded as an enumeration of names (or a successor function), starting e.g. from  $\ulcorner \mathbf{0} \urcorner$  for the name  $x_0$ , and then letting the name  $x_{i+1}$  be defined in terms of the name  $x_i$  as for example  $x_{i+1} \triangleq \ulcorner x_i \langle \mathbf{0} \rangle \urcorner$ . In the sequel, we shall say that  $\ulcorner x \langle \mathbf{0} \rangle \urcorner$  is a *left increment* of  $x$ , written  $+x$ . Then we can generate a countably infinite sequence of names  $x_0, x_1, x_2, \dots$ , starting from any name  $x = x_0$ , as  $+x = x_1, ++x = +x_1 = x_2, \dots$  and so on. This shows that the set of  $\pi$ -calculus names can be implemented as  $\rho$ -names, as, by the definition of name equivalence and structural congruence, we have that  $x \not\equiv_{\mathcal{N}} \ulcorner x \langle \mathbf{0} \rangle \urcorner$ .

Correspondingly we can define  $x+ \triangleq \ulcorner x \langle \ulcorner \mathbf{0} \urcorner \rangle . \mathbf{0} \urcorner$  as a *right increment* of  $x$ , which gives us another countably infinite sequence. Another option is *name composition*  $x \cdot y \triangleq \ulcorner x \langle \mathbf{0} \rangle \mid y \langle \ulcorner \mathbf{0} \urcorner \rangle . \mathbf{0} \urcorner$ , which yields yet another sequence with  $x^2 = x \cdot x, x^3 = x^2 \cdot x, x^4 = x^3 \cdot x, \dots$  and so on.

These are all examples of *static quoting* techniques for consistent name generation, and each could be used to implement the function  $\varphi$ . Given such techniques, Meredith and Radestock then begin by assuming that all  $\pi$ -calculus names are already implemented as  $\rho$ -names. Their translation function  $\llbracket P \rrbracket_{n_0, p_0}$  requires two names as parameters, which must be chosen such that they are distinct from all the names in  $P$ , and furthermore that no name *within*  $P$  can ever be *generated* from  $n_0$  or  $p_0$  by means of the aforementioned methods of static name generation. One way of ensuring this is by letting

$$n_0 = \ulcorner \prod_{x \in \text{fn}(P)} x \langle \mathbf{0} \rangle \urcorner \quad \text{and} \quad p_0 = \ulcorner \prod_{x \in \text{fn}(P)} x \langle \ulcorner \mathbf{0} \urcorner \rangle . \mathbf{0} \urcorner$$

where  $\prod$  denotes generalised parallel composition.

The translation function also uses two short-hands:  $D(x) \triangleq x(y).(\ulcorner y \urcorner \mid x \langle \ulcorner y \urcorner \rangle)$  is a copying process used to implement replication; and  $x\langle y \rangle \triangleq x \langle \ulcorner y \urcorner \rangle$  simulates output in the  $\pi$ -calculus, since by  $[\text{N-DRIP}]$

we have that  $\ulcorner \lrcorner y \lrcorner \urcorner \equiv_{\mathcal{N}} y$ . The translation  $\llbracket P \rrbracket = \llbracket P \rrbracket_{n_0, p_0}$  [11, p. 13] is then given by the following recursive equations:<sup>2</sup>

$$\begin{aligned} \llbracket \mathbf{0} \rrbracket_{n,p} &= \mathbf{0} & \llbracket P_1 \mid P_2 \rrbracket_{n,p} &= \llbracket P_1 \rrbracket_{+n,+p} \mid \llbracket P_2 \rrbracket_{n+,p+} \\ \llbracket \bar{x} \langle y \rangle \rrbracket_{n,p} &= x \langle y \rangle & \llbracket (\nu x) P \rrbracket_{n,p} &= p \langle x \rangle . \llbracket P \rrbracket_{+n,+p} \mid p \langle n \rangle \\ \llbracket x(y) . P \rrbracket_{n,p} &= x(y) . \llbracket P \rrbracket_{n,p} \\ \llbracket !P \rrbracket_{n,p} &= n \cdot p \langle n+(n) . p+(p) . (\llbracket P \rrbracket_{n,p} \mid D(n \cdot p) \mid n+ \langle n \langle n \rangle \rangle \mid p+ \langle p \langle p \rangle \rangle) \rangle \\ &\quad \mid D(n \cdot p) \mid n+ \langle +n \rangle \mid p+ \langle +p \rangle \end{aligned}$$

A central element in this translation is the encoding of replication,  $\llbracket !P \rrbracket_{n,p}$ , so we shall give some further details about its underlying intuitions. Firstly, with higher-order process mobility, we can create a diverging process simply as  $x \langle D(x) \rangle \mid D(x)$ . This construction is reminiscent of the  $\lambda$ -calculus  $\Omega$ -combinator  $(\lambda x.xx)\lambda x.xx$ :  $D(x)$  will run the process it receives on  $x$  whilst simultaneously making it available again on  $x$ , so by sending it a copy of  $D(x)$  itself, we obtain a process that continuously copies itself. Then, by embedding another process  $P$  in this construct,  $x \langle P \mid D(x) \rangle \mid D(x)$ , we obtain a process that will create arbitrarily many copies of  $P$  at runtime. Thus we can implement unguarded replication by using just a single name  $x$ . However, this name  $x$  must not be used by any other process, lest it might interfere with the replication. This is achieved in the above encoding by composing the two name parameters,  $n$  and  $p$ , to obtain a new name  $n \cdot p$ .

Secondly, if  $\llbracket P \rrbracket_{n,p}$  were simply copied in this fashion, any usage of the parameters  $n$  and  $p$  within the translation of  $P$  would also be copied, which thus could create a name clash. Therefore, the inner process is prefixed with two inputs that *bind*  $n$  and  $p$  within the continuation. In parallel, we then have two other processes,  $n+ \langle +n \rangle$  and  $p+ \langle +p \rangle$ , that output the new names  $+n$  and  $+p$ , which will be substituted for  $n$  and  $p$ . These processes are also copied, and in the next round of replication they will instead create the names  $\ulcorner +n \langle +n \rangle \urcorner$  and  $\ulcorner +p \langle +p \rangle \urcorner$ , and so on, thereby implementing a *runtime* form of name generation, similar to our static quoting technique.

For the purpose of defining a notion of behavioural equivalence that is comparable to that of other calculi that do feature a  $\nu$ -operator, Meredith and Radestock define a *name-restricted observation predicate*  $\downarrow^{\mathcal{N}}$  for the  $\rho$ -calculus, parametrised with a set of names  $\mathcal{N}$ . The idea is to only allow observation of names in this set. We follow their definition, but also allow the observation predicate to distinguish between input  $x$ , and output  $\bar{x}$ :<sup>3</sup>

$$[\rho\text{-BOUT}] \frac{x_1 \equiv_{\mathcal{N}} x_2 \quad x_1 \in \mathcal{N}}{x_1 \langle P \rangle \downarrow^{\mathcal{N}} \bar{x}_2} \quad [\rho\text{-BIN}] \frac{x_1 \equiv_{\mathcal{N}} x_2 \quad x_1 \in \mathcal{N}}{x_1(y) . P \downarrow^{\mathcal{N}} x_2} \quad [\rho\text{-BPAR}] \frac{P_1 \downarrow^{\mathcal{N}} \hat{x} \quad \vee \quad P_2 \downarrow^{\mathcal{N}} \hat{x}}{P_1 \mid P_2 \downarrow^{\mathcal{N}} \hat{x}}$$

where  $\hat{x}$  ranges over  $x, \bar{x}$ . An  $\mathcal{N}$ -restricted barbed bisimulation is then a symmetric, binary relation  $\mathcal{R}^{\mathcal{N}}$  on processes, parametrised with a set of names  $\mathcal{N}$ , such that  $(P_1, P_2) \in \mathcal{R}^{\mathcal{N}}$  implies:

- If  $P_1 \rightarrow P'_1$  then there exists a  $P'_2$  such that  $P_2 \rightarrow P'_2$  and  $(P'_1, P'_2) \in \mathcal{R}^{\mathcal{N}}$ .
- If  $P_1 \downarrow^{\mathcal{N}} \hat{x}$  then  $P_2 \downarrow^{\mathcal{N}} \hat{x}$ .

We say that  $P_1$  is  $\mathcal{N}$ -restricted barbed bisimilar to  $P_2$ , written  $\sim^{\mathcal{N}}$ , if there exists an  $\mathcal{N}$ -restricted barbed bisimulation  $\mathcal{R}^{\mathcal{N}}$  such that  $(P_1, P_2) \in \mathcal{R}^{\mathcal{N}}$ . The corresponding ‘weak’ observation predicate is then written

$$P \Downarrow^{\mathcal{N}} \hat{x} \triangleq \exists P' . P \rightarrow^* P' \wedge P' \downarrow^{\mathcal{N}} \hat{x}$$

<sup>2</sup>The translation has been adapted to use our notation for name increments, which we find more intuitive than  $x^l$  and  $x^r$ , which is used in the original presentation. We also use  $x \langle y \rangle$  rather than  $x[y]$  for output, which is more in line with standard  $\pi$ -calculus notation.

<sup>3</sup>The added distinction between input and output observations is only for use in our later development of a correct encoding, and does not invalidate our claim that the encoding by Meredith and Radestock is incorrect, since our counter-examples shall only rely on observing outputs.

where  $\rightarrow^*$  is the reflexive and transitive closure of  $\rightarrow$ , and by replacing  $P_2 \downarrow^{\mathcal{N}} \hat{x}$  with  $P_2 \Downarrow^{\mathcal{N}} \hat{x}$ , and  $P_2 \rightarrow P'_2$  with  $P_2 \rightarrow^* P'_2$  in the above definition, we obtain the corresponding notion of a *weak*  $\mathcal{N}$ -restricted barbed bisimulation. We say that  $P_1$  is *weakly*  $\mathcal{N}$ -restricted barbed bisimilar to  $P_2$ , written  $\approx^{\mathcal{N}}$ , if there exists a weak  $\mathcal{N}$ -restricted barbed bisimulation  $\mathcal{R}^{\mathcal{N}}$  that relates them.

The corresponding observation predicate for the  $\pi$ -calculus is built by the following rules for observation on output, restriction and replication

$$[\pi\text{-BOUT}] \frac{x \in \mathcal{N}}{\bar{x} \langle y \rangle \downarrow^{\mathcal{N}} \bar{x}} \quad [\pi\text{-BRES}] \frac{P \downarrow^{\mathcal{N}} \hat{x}}{(vz)P \downarrow^{\mathcal{N}} \hat{x}} \quad (x \neq z) \quad [\pi\text{-BREP}] \frac{P \downarrow^{\mathcal{N}} \hat{x}}{!P \downarrow^{\mathcal{N}} \hat{x}}$$

and with rules similar to  $[\rho\text{-BPAR}]$  and  $[\rho\text{-BIN}]$  in the  $\rho$ -calculus for observation on parallel composition and input, with strict syntactic equality replacing name equivalence in the premise of the latter rule. The notions of a weak observation predicate, and (strong resp. weak)  $\mathcal{N}$ -restricted barbed bisimulation and bisimilarity for the  $\pi$ -calculus are then defined as in the  $\rho$ -calculus. We write  $P \downarrow \hat{x}$ ,  $P \Downarrow \hat{x}$ ,  $P_1 \sim P_2$  and  $P_1 \approx P_2$  when  $\mathcal{N}$  is the set of all names, corresponding to no restriction on the names we can observe. This yields the familiar notions of (strong resp. weak) barbed bisimilarity in the  $\pi$ -calculus (as defined in e.g. [12]).

Given these notions of behavioural equivalence, Meredith and Radestock then state the following as a theorem [11, p. 14, Theorem 5.3], but without providing a proof:

$$P_1 \approx P_2 \iff \llbracket P_1 \rrbracket \approx^{\text{fn}(P_1) \cup \text{fn}(P_2)} \llbracket P_2 \rrbracket \quad (1)$$

with observation in the  $\rho$ -calculus restricted to  $\text{fn}(P_1) \cup \text{fn}(P_2)$ , i.e. the free names in  $P_1$  and  $P_2$ , implemented as  $\rho$ -names.<sup>4</sup>

## 4 The errors

We shall now see why the claim stated in 1 does not hold. Firstly, consider the following  $\pi$ -calculus processes:

$$P_1 \triangleq !(vz)\bar{u} \langle z \rangle \quad \text{and} \quad P_2 \triangleq (vz)!\bar{u} \langle z \rangle$$

Clearly, they represent different behaviours:  $P_2$  will continuously send out the *same* fresh name  $z$  on  $u$ , whilst  $P_1$  will send out *different* fresh names, as we can see by applying  $\alpha$ -conversion after unfolding the replication (see [10, p. 11] for details). We can also easily construct a testing context  $C$  such that they can be distinguished by the ( $\pi$ -calculus)  $\Downarrow \bar{x}$  predicate, for example

$$C \triangleq [ ] \mid u(n_1).u(n_2).(\bar{n}_1 \mid n_2.\bar{x})$$

where the objects for the input/output of  $\bar{n}_1, n_2$  and  $\bar{x}$  are ignored, as this only requires pure synchronisation. Clearly, if the two names received on  $u$  are the same, then  $n_1$  and  $n_2$  will be the same name, so they can synchronise and we will therefore be able to observe  $\bar{x}$  after 3 reduction steps. And conversely, if the two names are distinct, then we will not observe  $\bar{x}$ . Thus  $C[P_1] \Downarrow \bar{x}$  whilst  $C[P_2] \not\Downarrow \bar{x}$  as argued above.

Now we make a slight adjustment to the two terms. By composing an arbitrary process  $Q$  with the inner output process  $\bar{u} \langle z \rangle$  we obtain the following:

$$P'_1 \triangleq !((vz)\bar{u} \langle z \rangle \mid Q) \quad \text{and} \quad P'_2 \triangleq (vz)!(\bar{u} \langle z \rangle \mid Q)$$

<sup>4</sup>Note that the original presentation [11, p. 14, Theorem 5.3] only has  $P_1 \approx P_2 \iff \llbracket P_1 \rrbracket \approx^{\text{fn}(P_1)} \llbracket P_2 \rrbracket$ , but we regard this as a simple omission, since it trivially would not hold for the implication from right to left: Take for example  $P_1 \triangleq x \langle z \rangle$  and  $P_2 \triangleq x \langle z \rangle \mid w \langle z \rangle$ . Then we have that  $\text{fn}(P_1) = \{x\}$ , and indeed  $\llbracket P_1 \rrbracket \approx^{\{x\}} \llbracket P_2 \rrbracket$  since for  $i \in \{1, 2\}$  we have that  $\llbracket P_i \rrbracket \not\Downarrow$  and  $\llbracket P_i \rrbracket \Downarrow^{\{x\}} \bar{x}$ ; but obviously  $P_1 \not\approx P_2$ , since  $P_2 \downarrow \bar{w}$  but  $P_1 \not\downarrow \bar{w}$ .

The actual behaviour of  $Q$  is irrelevant; it is there solely to induce the parameter pair  $(n, p)$  to be split into a ‘left pair’  $(+n, +p)$  and a ‘right pair’  $(n+, p+)$  that are passed to the translations of the left (resp. right) parts of the parallel composition. Note also that this changes nothing w.r.t. observability of  $\bar{x}$ : we still have that  $C[P'_1] \not\Downarrow \bar{x}$  and  $C[P'_2] \Downarrow \bar{x}$ .

We shall now perform the actual translation. To make it more readable, we tabulate the names generated by static quoting during the translation and rename them as follows:

$$\begin{array}{l} n \cdot p = a \quad p+ = c \quad +p = e \quad (+p)+ = g \quad ++n = i \\ n+ = b \quad +n = d \quad (+n)+ = f \quad (+n) \cdot (+p) = h \quad ++p = j \end{array}$$

Note that *none* of these names will be observable by the  $\Downarrow^{\text{fn}(P_1) \cup \text{fn}(P_2)}$  predicate, because they are generated by the translation, and hence are not in the set  $\text{fn}(P_1) \cup \text{fn}(P_2)$  of free names of  $P_1$  and  $P_2$ . Now, here is the translation:

$$\begin{aligned} \llbracket P'_1 \rrbracket_{n,p} &= a \left\langle b(n) \cdot c(p) \cdot \left( e(z) \cdot u\langle z \rangle \mid e\langle d \rangle \mid \llbracket Q \rrbracket_{f,g} \mid D(a) \mid b\langle n\langle n \rangle \rangle \mid c\langle p\langle p \rangle \rangle \right) \right\rangle \\ &\quad \mid D(a) \mid b\langle d \rangle \mid c\langle e \rangle \\ \llbracket P'_2 \rrbracket_{n,p} &= p(z) \cdot h \left\langle f(d) \cdot g(e) \cdot \left( u\langle z \rangle \mid \llbracket Q \rrbracket_{f,g} \mid D(h) \mid f\langle d\langle d \rangle \rangle \mid g\langle e\langle e \rangle \rangle \right) \right\rangle \\ &\quad \mid D(h) \mid f\langle i \rangle \mid g\langle j \rangle \mid p\langle n \rangle \end{aligned}$$

By performing the reductions, we see (not surprisingly) that  $\llbracket P'_2 \rrbracket_{n,p}$  firstly performs the communication on  $p$ , which causes  $z$  to be replaced by  $n$ , and the process afterwards expands into arbitrarily many instances of  $u\langle n \rangle$  (see [10, p. 12] for a reduction sequence). On the other hand, the translated process  $\llbracket P'_1 \rrbracket_{n,p}$  will immediately go through the replication steps, thereby creating arbitrarily many instances of the process  $e(z) \cdot u\langle z \rangle \mid e\langle d \rangle$  corresponding to the translation of  $(vz)\bar{u}\langle z \rangle$ . This process obviously reduces to  $u\langle d \rangle$  in one step. However, precisely because of the aforementioned split of  $(n, p)$  over the translation of parallel composition, the name  $d$  will *not* be updated by the replication context. This process will therefore *also* repeatedly output the *same* name  $d$  on  $u$ , and the (translated) form of our testing context can therefore no longer distinguish the processes.

Both  $\llbracket P'_1 \rrbracket$  and  $\llbracket P'_2 \rrbracket$  thus reduce to arbitrarily many copies of either  $u\langle d \rangle$  (for  $P'_1$ ) or  $u\langle n \rangle$  (for  $P'_2$ ), and  $u$  is the only name we can observe, as all the other names are created by the translation. This then gives us our desired counter-example: by also translating the testing context we obtain a pair of processes where

$$C[P'_1] \not\approx C[P'_2] \quad \text{but} \quad \llbracket C[P'_1] \rrbracket \approx^{\text{fn}(C[P'_1]) \cup \text{fn}(C[P'_2])} \llbracket C[P'_2] \rrbracket$$

in contradiction of the implication from right to left in the claim stated in 1.

The detailed analysis above gives us a clear idea of the root cause of the problem: The translation of replication creates a context with the purpose of ensuring that the names  $(n, p)$  used within it will repeatedly be substituted with new, fresh names  $(+n, +p)$  dynamically built from the previous names, and these act as sources of new names for any occurrence of  $(vz)P$  within a replicated process. The point is precisely to ensure that each instance of a replicated  $v$  operator will generate a unique new name, and the parameters  $(n, p)$  on the translation function act as ‘handles’ to access this resource; they are the names that have *most recently* been replicated.

The problem arises because this property of being the ‘most recently replicated names’ is not preserved by the translation of parallel composition: It splits the pair into a left and a right pair, used in the translation of the left and right parallel components:

$$\llbracket P_1 \mid P_2 \rrbracket_{n,p} = \llbracket P_1 \rrbracket_{+n,+p} \mid \llbracket P_2 \rrbracket_{n+,p+}$$

Thus, the access to the most recently replicated names is lost in the translation of the inner processes, because, as we noted above, substitution does *not* recur into processes under quotes. Therefore, when the replication context increments  $(n, p)$  at runtime, this update cannot touch the  $n$  and  $p$  embedded in the *statically* incremented names  $(+n, +p)$  and  $(n+, p+)$  which the translation function generates for the translation of parallel composition. This is why we added an arbitrary  $Q$  to create a parallel composition in our counter-example above.

However, the error above is not the only one in the claim by Meredith and Radestock: whilst its root cause was the splitting of names over the translation of parallel composition, we can also create another example that is more directly related to the interplay between  $(\nu x)P$  and replication. Consider the following processes:

$$P_1 \triangleq !(\nu z)\bar{u}\langle z \rangle \quad \text{and} \quad P_2 \triangleq !(\nu q)(\nu z)\bar{u}\langle z \rangle$$

Note that  $P_1$  and  $P_2$  are structurally congruent, since the new name  $q$  is never used. Thus  $P_1 \approx P_2$  also holds. Yet when we translate those terms, the name incrementation in the translation of a term of the form  $(\nu x)P$  means that we again lose access to the most recently replicated names from the translation of replication. This can be easily seen if we perform the translation stepwise, using the same tabulated list of names as before. For both processes, the translation of replication is the same:

$$\llbracket !P \rrbracket_{n,p} = a \langle b(n) . c(p) . (\llbracket P \rrbracket_{n,p} \mid D(a) \mid b \langle n \langle n \rangle \rangle \mid c \langle p \langle p \rangle \rangle) \rangle \mid D(a) \mid b \langle d \rangle \mid c \langle e \rangle$$

Now let  $P'_1 \triangleq (\nu z)\bar{u}\langle z \rangle$  and  $P'_2 \triangleq (\nu q)(\nu z)\bar{u}\langle z \rangle$  and replace  $\llbracket P \rrbracket_{n,p}$  above with  $\llbracket P'_1 \rrbracket_{n,p}$  and  $\llbracket P'_2 \rrbracket_{n,p}$  respectively. The translations of the inner processes yield:

$$\begin{aligned} \llbracket (\nu z)\bar{u}\langle z \rangle \rrbracket_{n,p} &= p \langle z \rangle . u \langle z \rangle \mid p \langle n \rangle \\ \llbracket (\nu q)(\nu z)\bar{u}\langle z \rangle \rrbracket_{n,p} &= p \langle q \rangle . (e \langle z \rangle . u \langle z \rangle \mid e \langle d \rangle) \mid p \langle n \rangle \end{aligned}$$

which reduce to  $u \langle n \rangle$  and  $u \langle d \rangle$  respectively. The names  $n, p$  are bound in the replication context and will therefore be updated whenever the process replicates. However, in the case of  $P_2$ , these names are *statically* incremented in the translation of  $(\nu q)$  to yield the names  $+n = d$  and  $+p = e$ , and these two names will therefore *not* be updated at runtime, just as in the previous counter-example. Consequently, in the case of  $P_2$  the names sent out on  $u$  will *not* be distinct; they will all be the name  $+n = d$ . We can therefore use the same testing context  $C$  as in the previous example and proceed as before to generate another contradiction of the claim in 1; this time by *distinguishing* the translated terms, although we have  $C[P_1] \approx C[P_2]$  in the  $\pi$ -calculus. In summary, neither of the implications in the claim stated in 1 hold.

## 5 Our criteria for encodability

Both of the previous examples illustrate the difficulties involved in reasoning about a parametrised translation. Usually, the parameters represent a property or invariant that is assumed to be preserved throughout the translation, and a proof of correctness of the translation must therefore also include a proof that this invariant or property is indeed preserved. For example, in the present case, the invariant assumed to hold for the parameters is precisely that they always refer to the most recently replicated names. However, this assumption is never formally stated in the original  $\rho$ -calculus paper [11], and as the examples above show, it does not hold either. Thus, a naive attempt to show correctness of the translation by induction in the clauses of the translation function may therefore seemingly go through, if the parameters are not considered. This is doubly problematic in the present case, because the observation predicate used



in the bisimulation relation over  $\rho$ -calculus terms is parametrised so that we do *not* observe the names created by the translation function.

Full abstraction, of which the claim in 1 is an instance, may also not be the most informative correctness criterion, as argued by Gorla and Nestmann [9]; for example, it does not necessarily prevent the translation from introducing divergence. Also, as we are here more interested in showing that the  $\pi$ -calculus is ‘implementable’ in the  $\rho$ -calculus than in transferring equations between the source and target language, we shall instead follow the approach of such authors as Gorla [8], Carbone and Maffei [4] and others, and state a number of criteria for what we consider a valid encoding, where we also take the presence of parameters into account:

**Definition 1** (Language). A language  $\mathcal{L}$  is a tuple  $\mathcal{L} \triangleq (\mathcal{P}, \mathcal{N}, \rightarrow, \simeq)$ , where  $\mathcal{P}$  is a set of terms,  $\mathcal{N}$  is a set of names,  $\rightarrow \subseteq \mathcal{P} \times \mathcal{P}$  is the reduction relation, with  $\rightarrow^*$  denoting the reflexive and transitive closure of  $\rightarrow$ , and  $\simeq \subseteq \mathcal{P} \times \mathcal{P}$  is a notion of behavioural equivalence.

We say a term  $P \in \mathcal{P}$  *diverges*, written  $P \rightarrow^\omega$ , if  $P$  has an infinite reduction sequence. We use  $\sigma : \mathcal{N} \rightarrow \mathcal{N}$  to denote a substitution function in  $\mathcal{L}$ . For encodings, we need the notion of a *source* and a *target* language, and we shall generally use the convention of subscripting  $s$  (for source) and  $t$  (for target) to a language  $\mathcal{L}$  or its components, including substitutions, and we let  $S \in \mathcal{P}_s$  and  $T \in \mathcal{P}_t$ .

**Definition 2** (Encoding). An encoding of  $\mathcal{L}_s$  into  $\mathcal{L}_t$  is a tuple  $(\llbracket \cdot \rrbracket_N, \varphi, \delta)$ , where  $\llbracket \cdot \rrbracket_N : \mathcal{P}_s \rightarrow \mathcal{P}_t$  is a translation function, parametrised with a finite list of names  $N \in \mathcal{N}_t^k$ ; and  $\varphi : \mathcal{N}_s \rightarrow \mathcal{N}_t$  is a renaming policy, mapping names in the source language into names in the target language; and  $\delta : \mathcal{N}_t^k \rightarrow \mathcal{N}_t^k$  is a name derivation function, mapping  $k$ -ary tuples of target names to tuples of equal arity for some  $k$ .

The name derivation function  $\delta$  allows us to express that the list of name parameters  $N$  may evolve in some predictable way during the course of translation. This seems necessary in particular when we are working with a language with structured terms as names. In some cases we may also need to derive multiple tuples of names from the same input tuple; thus to comply with the requirement that  $\delta$  is a single function, we could e.g. envision using an extra, designated name as argument to control the derivation method used by  $\delta$ . However, to abstract away from such details, we say that a tuple of names  $N_2$  is *derivable* from some tuple of names  $N_1$ , written  $N_1 \rightsquigarrow N_2$ , if  $\delta(N_1) = N_2$ , and likewise that  $N_1 \rightsquigarrow n$  if  $n \in N_2$ . Note that we abuse the notation slightly and treat the lists as sets when the position of each individual component does not matter.

**Definition 3** (Valid encoding). We shall regard an encoding as valid, if it satisfies at least the following criteria:

1. *Compositionality*:  $\llbracket S_1 \mid \dots \mid S_n \rrbracket_N = C \mid \llbracket S_1 \rrbracket_{N_1} \mid \dots \mid \llbracket S_n \rrbracket_{N_n}$  where  $C$  is an optional coordinating context and  $\text{fn}(C) \subseteq \varphi(\text{fn}(S_1 \mid \dots \mid S_n)) \cup N$ , and for each  $i \in \{1, \dots, n\}$  we have that  $N \rightsquigarrow N_i$ .
2. *Substitution invariance*:  $\llbracket S\sigma_s \rrbracket_N \simeq \llbracket S \rrbracket_N \sigma_t$  for each  $\sigma_s$ , where  $\varphi(\sigma_s(x)) = \sigma_t(\varphi(x))$ .
3. *Operational correspondence*:  $S \rightarrow^* S' \iff \exists T' . \llbracket S \rrbracket_N \rightarrow^* T' \wedge T' \simeq \llbracket S' \rrbracket_{N'}$  and  $N \rightsquigarrow N'$ .
4. *Observational correspondence*: We require that  $N \cap \varphi(\mathcal{M}) = \emptyset$  for any set of observable names  $\mathcal{M}$ . Then  $P \downarrow^{\mathcal{M}} \hat{x} \iff \llbracket P \rrbracket_N \downarrow^{\varphi(\mathcal{M})} \varphi(\hat{x})$ .
5. *Divergence reflection*:  $\llbracket P \rrbracket_N \rightarrow^\omega \implies P \rightarrow^\omega$ .
6. *Parameter independence*:  $\llbracket P \rrbracket_{N_1} \simeq \llbracket P \rrbracket_{N_2}$  for each finite  $N_1, N_2$ .

These criteria are very close to those proposed by Gorla [8], except that we have chosen observational correspondence, rather than the less specific success testing; i.e.  $P \rightarrow^* \downarrow \checkmark$  implies  $\llbracket P \rrbracket_N \rightarrow^* \downarrow \checkmark$ . This

can easily be obtained, simply by choosing a specific name  $x$  and then defining  $\checkmark$  as a process with  $x$  in subject position, as we did in our counter-examples above.

Furthermore, as we are here allowing parameters to appear on the translation, we have also added the criterion of parameter independence, which does not appear in [8]. This is just to ensure that the behaviour of the translated terms will not depend on the exact choice of the parameters. Likewise, we have also added name restriction to the observation predicate for observational correspondence  $\Downarrow^{\mathcal{M}}$ , and we require that  $N \cap \mathcal{M} = \emptyset$ ; i.e. that the parameters should not be observable. This seems a natural requirement, since we also require that  $N \subseteq \mathcal{N}_t$ ; i.e. that the parameters belong to the target language. They should therefore not be observable on the source terms.

## 6 A correct encoding

As the previous examples have illustrated, the main difficulty in creating an encoding of the  $\pi$ -calculus in the  $\rho$ -calculus, is how to achieve a robust source of fresh names at runtime that are guaranteed never to cause a name clash. One way is to use a dedicated process for this purpose. Consider the following process, where  $D(x)$  is defined as in section 3:

$$!N(x, z, v, s) \triangleq D(x) \mid x \left\langle z(a) \cdot v(r) \cdot \left( D(x) \mid r \langle \ulcorner a \urcorner \rangle \mid z \langle a \langle \mathbf{0} \rangle \rangle \right) \right\rangle \mid z \langle \ulcorner s \urcorner \rangle$$

This process is a *name server*; it consistently generates names corresponding to consecutive left-increments of the initial name  $s$  and outputs them on the ‘return address’  $r$  received on  $v$ . We refer to the above form as the *initial state* of the name server and note that after two reductions it evolves to the form

$$v(r) \cdot \left( D(x) \mid r \langle \ulcorner s \urcorner \rangle \mid z \langle \ulcorner \ulcorner s \urcorner \urcorner \langle \mathbf{0} \rangle \rangle \right) \mid x \left\langle z(a) \cdot v(r) \cdot \left( D(x) \mid r \langle \ulcorner a \urcorner \rangle \mid z \langle a \langle \mathbf{0} \rangle \rangle \right) \right\rangle$$

which we refer to as its *ready state*, where it blocks, awaiting a request for a new name on  $v$ . The first request will return  $\ulcorner \ulcorner s \urcorner \urcorner$ ; a second request will return  $\ulcorner \ulcorner \ulcorner s \urcorner \urcorner \langle \mathbf{0} \rangle \urcorner = +s$ , and so on.

We can verify that the names will all be distinct by considering the *quote depth* of a name (resp. process) defined thus:

$$\text{QD}(\ulcorner P \urcorner) = \begin{cases} \text{QD}(x) & \text{if } P \equiv \ulcorner x \urcorner \\ 1 + \text{QD}(P) & \text{otherwise} \end{cases} \quad \text{QD}(P) = \begin{cases} \max \{ \text{QD}(x) \mid x \in \text{fn}(P) \} & \text{if } \text{fn}(P) \neq \emptyset \\ 0 & \text{otherwise} \end{cases}$$

The quote depth of a name  $x_1$  corresponds to the maximum number of calls to [N-STRUCT] used to conclude name equivalence  $x_1 \equiv_{\mathcal{N}} x_2$  for some name  $x_2$ . Thus, a necessary (but not sufficient) condition for two names to be name equivalent is that they have the same quote depth. Names are therefore automatically stratified based on their quote depth:

**Lemma 1** (Stratification).  $x_1 \equiv_{\mathcal{N}} x_2 \implies \text{QD}(x_1) = \text{QD}(x_2)$ .

We can also partition names into *namespaces* in the following way: let  $\mathcal{N}_{[\ ]}$  be a collection of name contexts, ranged over by  $N$ , with one or more holes occurring in the position of free names. If  $s$  is a name, then so is  $N[s]$  for some  $N \in \mathcal{N}_{[\ ]}$ . We write  $\mathcal{N}_{[s]} \triangleq \{ N[s] \mid N \in \mathcal{N}_{[\ ]} \}$ , and we say that  $\mathcal{N}_{[s]}$  is a *namespace rooted at  $s$* . Clearly, if  $\text{QD}(N) = n$  (counting  $\text{QD}([\ ]) = 0$ ), and  $\text{QD}(s) = i$  and  $\text{QD}(s') = j$ , then  $\text{QD}(N[s]) = n + i$  and  $\text{QD}(N[s']) = n + j$ .

Using the concepts of name contexts, we can describe our aforementioned three static quoting techniques as three distinct name space ‘templates,’ built by the following grammars:

$$\begin{aligned} \ulcorner N \in \mathcal{N}_{[\ ]}^+ ::= [\ ] \mid \ulcorner^+ N \langle \mathbf{0} \rangle \urcorner \\ N^+ \in \mathcal{N}_{[\ ]}^+ ::= [\ ] \mid \ulcorner N^+ (\ulcorner \mathbf{0} \urcorner) \cdot \mathbf{0} \urcorner \\ N^\circ \in \mathcal{N}_{[\ ]}^\circ ::= [\ ] \mid \ulcorner N^\circ \langle \mathbf{0} \rangle \mid N^\circ (\ulcorner \mathbf{0} \urcorner) \cdot \mathbf{0} \urcorner \end{aligned}$$

We shall use these namespace templates to implement the name derivation function  $\delta$ . Thus, if we let  $\widehat{N}$  denote any of the name contexts  ${}^+N, N^+, N^o$  then  $s \rightsquigarrow s'$  if there exists a name context  $\widehat{N}$  such that  $s' \equiv_{\neq} \widehat{N}[s]$ . This assures us that even if two namespaces use the same structure, e.g.  $\mathcal{N}_{[ ]}$ , all their names will still be distinct *if* their roots are not name equivalent, and neither is derivable from the other.

In case of the name server, we see that it generates the namespace  $\mathcal{N}_{[s]}$ , i.e. the namespace of left-increments rooted at  $s$ , where  $s$  is a parameter. Thus if  $s_1 \not\equiv_{\neq} s_2$  and neither is derivable from the other, then  $!N(x, z, v, s_1)$  and  $!N(x, z, v, s_2)$  will generate similarly structured namespaces,  $\mathcal{N}_{[s_1]}$  and  $\mathcal{N}_{[s_2]}$ , but consisting of different sets of names. Yet we can easily construct a mapping  $\mathcal{N}_{[s_1]} \mapsto \mathcal{N}_{[s_2]}$  simply by replacing  $s_1$  with  $s_2$  within each name  ${}^+N[s_1] \in \mathcal{N}_{[s_1]}$ . This will be important in the proof for parameter independence below.

Based on these considerations we can now construct our encoding. We let the encoding be defined as  $\llbracket P \rrbracket \triangleq \llbracket P \rrbracket_{n,v} \mid !N(x, z, v, s)$ , where we assume we can choose the names  $n, v, x, z, s$  such that they are distinct from all free names in  $P$  and  $n, v, x, z \notin \mathcal{N}_{[s]}$ . As in the encoding by Meredith and Radestock, we shall assume that all  $\pi$ -calculus names are implemented as  $\rho$ -names, and thus we shall generally omit explicit reference to  $\varphi$  in the following. We shall also limit ourselves to the  $\pi$ -calculus fragment with only input-guarded replication, to ensure that the encoding does not introduce divergence, unlike the encoding by Meredith and Radestock which replicates eagerly and therefore always diverges.<sup>5</sup> This can be achieved by prefixing the object of the lift with an input construct, i.e.  $n \langle x(y) \cdot (D(n) \mid P) \rangle$ , since

$$D(n) \mid n \langle x(y) \cdot (D(n) \mid P) \rangle \rightarrow x(y) \cdot (D(n) \mid P) \mid n \langle x(y) \cdot (D(n) \mid P) \rangle$$

and the process then blocks until it receives a communication on  $x$ . Given these considerations, the translation function  $\llbracket \cdot \rrbracket_{n,v}$  is then given by the following equations:

$$\begin{aligned} \llbracket \mathbf{0} \rrbracket_{n,v} &= \mathbf{0} & \llbracket \bar{x}\langle z \rangle \rrbracket_{n,v} &= x\langle z \rangle \\ \llbracket P_1 \mid P_2 \rrbracket_{n,v} &= \llbracket P_1 \rrbracket_{+n,v} \mid \llbracket P_2 \rrbracket_{n+,v} & \llbracket (vx)P \rrbracket_{n,v} &= v\langle n \rangle \mid n(x) \cdot \llbracket P \rrbracket_{n-n,v} \\ \llbracket x(y) \cdot P \rrbracket_{n,v} &= x(y) \cdot \llbracket P \rrbracket_{n,v} & \llbracket !x(y) \cdot P \rrbracket_{n,v} &= D(n) \mid n \langle x(y) \cdot (D(n) \mid \llbracket P \rrbracket_{n-n,v}) \rangle \end{aligned}$$

The idea is that we simplify the ‘bookkeeping’ involved in runtime name generation by isolating it to a single, contextual process. This prevents errors of the first kind in the encoding by Meredith and Radestock, which resulted from processes losing access to the most recently replicated names. Here, the name  $v$  is used by all processes to contact the name server, and since it is never updated this access can never be lost. Conversely, the name  $n$ , which is used for the ‘return address,’ as well as for replication, is *always* updated incrementally, during the translation. It is never bound or reused, unlike in the translation by Meredith and Radestock, where the replication context used  $+n, +p$  but also bound  $n, p$  and passed them to the inner translation of  $P$ , which resulted in the second kind of error. We say that a name is *unique for the translation* if it is never generated more than once by the translation function, and this is the invariant that should hold for the parameter  $n$ :

**Lemma 2 (Uniqueness).** *For each clause  $\llbracket C[P] \rrbracket_{n,v} = \llbracket C \rrbracket_{n,v} [\llbracket P \rrbracket_{n',v}]$ , where  $n \rightsquigarrow n'$ , and  $\llbracket C \rrbracket_{n,v}$  contains a set of names  $N' = \{n_1, \dots, n_k\}$  such that  $n \rightsquigarrow N'$ , it holds that if  $n$  is unique for the translation, then so are  $n_1, \dots, n_k$  and  $n'$ .*

This can easily be shown by examining the clauses of the translation function, assuming  $n$  is unique. For every usage of  $n$  in a clause, we always either increase the quote depth of the parameter we pass to the inner call to the translation, or we shift the parameter into a new namespace by composition. Furthermore, the behaviour of the translated process does not depend on the structure of the name parameter  $n$ , as long as  $n$  is unique:

<sup>5</sup>This is only a slight limitation, as we can use input-guarded replication to encode full replication. Note also that having only input-guarded replication would not have prevented any of the errors described in section 4.

**Proposition 1** (Independence of parameters). *If  $n, n', s, s' \# n(P)$  and all are unique for the translation, then  $\llbracket P \rrbracket_{n,v} \mid !N(x, z, v, s) \sim^{\text{fn}(P)} \llbracket P \rrbracket_{n',v} \mid !N(x, z, v, s')$ .*

This follows from the fact that the translation only generates finitely many names, say, of the structure  $\mathcal{N}_{[\ ]}$ , so we can construct a finite substitution  $\sigma_t : \mathcal{N}_{[n]} \rightarrow \mathcal{N}_{[n']}$  and simply apply it to  $\llbracket P \rrbracket_{n,v}$  to obtain  $\llbracket P \rrbracket_{n',v}$ . Then as we know that  $n, n', s, s' \# n(P)$ , and by construction  $x \notin \text{fn}(P)$  for each  $x \in \mathcal{N}_{[s]} \cup \mathcal{N}_{[s']}$ , none of these names can be observed by the  $\downarrow^{\text{fn}(P)}$  predicate, so they cannot be used to distinguish the two processes. A similar argument can then be made for the name server and the two namespaces  $\dagger\mathcal{N}_{[s]}$  and  $\dagger\mathcal{N}_{[s']}$  generated by it at runtime.

Next, we formulate a (mostly) standard result relating substitution in the two calculi:

**Proposition 2** (Substitution). *Let  $\sigma_s \triangleq \{u/w\}$  denote substitution in the  $\pi$ -calculus, and let  $\sigma_t \triangleq \{u/w\}$  denote substitution in the  $\rho$ -calculus. Then  $\llbracket P\sigma_s \rrbracket_{n,v} = \llbracket P \rrbracket_{n,v}\sigma_t$  if  $u, w \# P, n, v, \mathcal{N}_{[n]}$ .*

This is proved by induction in the clauses of the translation. The condition  $u, w \# P, n, v, \mathcal{N}_{[n]}$  ensures that the substitution cannot touch any of the names created by the translation, which is reasonable, since the substitutions we care about should derive from communications in the  $\pi$ -calculus, and not from some of the ‘internal’ reductions in the  $\rho$ -calculus that are used to simulate replication or requests for new names.

Our next result establishes that our translation preserves observability of subjects, as long as we restrict observations to the set of free names in  $P$ :

**Proposition 3** (Weak observational correspondence). *Let  $\Downarrow^{\mathcal{N}}$  be the least predicate such that  $\llbracket S \rrbracket \Downarrow^{\mathcal{N}} \hat{n}$  holds if either of the following conditions are satisfied:*

1. *if  $S = S_1 \mid S_2$  and  $\llbracket S_1 \rrbracket \Downarrow^{\mathcal{N}} \hat{n} \vee \llbracket S_2 \rrbracket \Downarrow^{\mathcal{N}} \hat{n}$*
2. *if  $S \neq S_1 \mid S_2$  and  $\llbracket S \rrbracket_{n,v} \mid !N(x, z, v, s) \rightarrow^* T' \wedge T' \Downarrow^{\mathcal{N}} \hat{n}$*

*Then for any  $x$ ,  $P \Downarrow^{\text{fn}(P)} \hat{x} \iff \llbracket P \rrbracket \Downarrow^{\text{fn}(P)} \hat{x}$ .*

This is proved by induction in the clauses of the translation. Note that we purposefully restrict the weak observation predicate to only allow reductions involved in replication and requesting a fresh name from the name server; i.e. by splitting it directly over parallel compositions rather than allowing them to first interact. This is necessary for proving the implication from right to left in Proposition 3, since reductions might otherwise expose more names that are not immediately observable in the source terms. This restriction can be lifted if we replace  $\downarrow$  by  $\Downarrow$  in the  $\pi$ -calculus, but we prefer this slightly more complicated formulation to illustrate that observability is strictly preserved, in the sense that any auxiliary steps required in the  $\rho$ -calculus are ‘internal,’ deriving either from a replication step, a request for a new name, or from the name server as it moves from its initial state to its ready state, and neither of these are observable by the  $\downarrow^{\text{fn}(P)}$  predicate.

Next we show that the translation preserves the semantic meaning of the source program:

**Proposition 4** (Operational correspondence).  *$P \rightarrow^* P' \iff \llbracket P \rrbracket \rightarrow^* \approx^{\text{fn}(P)} \llbracket P' \rrbracket$ .*

This proof can be split into two parts. For the forward direction (completeness) we can actually show the stronger statement that  $P \rightarrow P' \implies \llbracket P \rrbracket \rightarrow \rightarrow^* \approx^{\text{fn}(P)} \llbracket P' \rrbracket$  by induction in the reduction semantics of the  $\pi$ -calculus, as every reduction in the  $\pi$ -calculus is matched by one or more steps in the  $\rho$ -calculus. The proof often relies on Proposition 2 for the cases of communication, replication and  $(vx)P$ , and on Proposition 1 when we translate the reduct of the  $\pi$ -calculus term as this often induces a slightly different form on the parameters.

For the other direction (soundness) we can only prove the weaker form  $\llbracket P \rrbracket \rightarrow^* T' \implies \exists P'. P \rightarrow^* P' \wedge T' \approx^{\text{fn}(P)} \llbracket P' \rrbracket$ , due to the extra reductions deriving from the name server, replication, or requests for

new names. Thus we proceed by induction in the reduction sequence, and often again making use of Proposition 1.

Having only the weaker form of completeness, with  $\rightarrow^*$  instead of  $\rightarrow$ , of course means that this statement in itself is not enough to verify that the translation does not introduce divergence. We therefore prove this separately:

**Proposition 5** (Divergence reflection).  $\llbracket P \rrbracket \rightarrow^\omega \implies P \rightarrow^\omega$ .

We show this by induction in the clauses of the translation function. The matter is made easier by the fact that a reduction sequence related to the name server, requests for new names, or unfolding replication, is always of finite length: the name server takes two steps to evolve from its initial state to its ready state, where it blocks until it receives a request; serving a request requires two steps, and then two further steps to return to its ready state; and input-guarded replication takes a single step to unfold once, after which it blocks until it receives an input.

## 7 A separation result

The  $\rho$ -calculus can encode the  $\pi$ -calculus, as we saw in the previous section. However, the converse does not hold. Under some general assumptions about the behavioural equivalence  $\simeq$  used in the target language, we can show that there cannot be an encoding of the  $\rho$ -calculus into the  $\pi$ -calculus that satisfies our validity criteria from Definition 3. This result relies on a simple observation about substitution in the  $\pi$ -calculus, namely that reduction is preserved under substitution:

**Lemma 3.** *Let  $\sigma_t = \{x/n\}$  be a substitution in the  $\pi$ -calculus, with  $n \in \text{fn}(P)$  and  $x \# P$ . Then  $P \rightarrow P' \implies P\sigma_t \rightarrow P'\sigma_t$ .*

This can easily be shown by induction in the semantic rules, and then with an extra induction in structural congruence for the  $[\pi\text{-STRUCT}]$  rule.

Next, we consider our requirements for the notion of behavioural equivalence: First of all,  $\simeq$  should obviously be an equivalence relation. Secondly, it should in some sense preserve the semantics of the processes it equates: as we are here working in a reduction system, it should at least preserve reductions and observability, and it should be preserved under substitution:

**Definition 4** (Behavioural equivalence requirements). *We require that  $\simeq$  be at least an equivalence relation over  $\pi$ -terms satisfying the following:*

1.  $P_1 \simeq P_2 \wedge P_1 \rightarrow^* P'_1 \implies \exists P'_2. P_2 \rightarrow^* P'_2 \wedge P'_1 \simeq P'_2$
2.  $P_1 \simeq P_2 \wedge P_1 \Downarrow \hat{x} \implies P_2 \Downarrow \hat{x}$
3.  $P_1 \simeq P_2 \implies P_1\sigma_t \simeq P_2\sigma_t$

The requirements suggest that  $\simeq$  should be at least weak, barbed congruence, which does not seem too demanding. However, we prefer to keep the formulation general, without committing to one specific notion of behavioural equivalence, to emphasise that other, stronger choices are also possible. The following result will then hold for any such choice:

**Theorem 1** (Separation). *If  $\simeq$  satisfies the requirements of Definition 4, then there is no encoding of the  $\rho$ -calculus into the  $\pi$ -calculus satisfying the criteria of Definition 3.*

*Proof.* Assume to the contrary that there exists a translation  $\llbracket \cdot \rrbracket_N : \mathcal{P}_\rho \rightarrow \mathcal{P}_\pi$  satisfying the criteria of Definition 3. We show that this leads to a contradiction. Firstly, let  $u \triangleq \ulcorner x_1 \urcorner \mid \ulcorner x_2 \urcorner$ , and consider the processes  $P$  and  $P'$  where

$$P \triangleq P_1 \mid P_2 \quad P_1 \triangleq a \langle \ulcorner x_1 \urcorner \mid \ulcorner x_2 \urcorner \rangle \quad P_2 \triangleq a(n).n \langle \mathbf{0} \rangle \quad P' \triangleq u \langle \mathbf{0} \rangle$$

Thus  $P = a \langle \ulcorner x_1 \urcorner \mid \ulcorner x_2 \urcorner \rangle \mid a(n).n \langle \mathbf{0} \rangle$  and clearly  $P \not\Downarrow u$  and  $u \notin \text{fn}(P)$ , but  $P \rightarrow \ulcorner \ulcorner x_1 \urcorner \mid \ulcorner x_2 \urcorner \urcorner \langle \mathbf{0} \rangle = u \langle \mathbf{0} \rangle = P'$  and  $P' \Downarrow u$ .

Consider now the substitution  $\sigma_t \triangleq \{m/\varphi(u)\}$  for some fresh name  $m$ , i.e.  $m \neq \varphi(u)$  and with  $m \notin \text{fn}(\llbracket P \rrbracket_N)$ .  $P \rightarrow P'$  gives, by criterion 3 (operational completeness), that  $\llbracket P \rrbracket_N \rightarrow^* T'$  and  $T' \simeq \llbracket P' \rrbracket_{N'}$  for some  $T'$  and  $N'$  derivable from  $N$ . By criterion 2 (substitution invariance),  $\sigma_t(\varphi(u)) = m$  implies  $\exists \sigma_s. \varphi(\sigma_s(u)) = m$ , so we can combine  $\sigma_s$  with the observability predicate. By criterion 4 (observational correspondence), since  $P' \not\Downarrow \sigma_s(u)$ , we therefore also have that  $\llbracket P' \rrbracket_{N'} \not\Downarrow m$ . This establishes that

$$\llbracket P \rrbracket_N \rightarrow^* T' \wedge T' \simeq \llbracket P' \rrbracket_{N'} \wedge \llbracket P' \rrbracket_{N'} \not\Downarrow m$$

as expected. By requirement 2 in Definition 4, since  $\llbracket P' \rrbracket_{N'} \simeq T'$ , it must therefore also be the case that  $T' \not\Downarrow m$ , and hence that  $\llbracket P \rrbracket_N \not\Downarrow m$ .

Now consider the term  $\llbracket P \rrbracket_N \sigma_t$ : Lemma 3 yields  $\llbracket P \rrbracket_N \sigma_t \rightarrow^* T' \sigma_t \simeq \llbracket P' \rrbracket_{N'} \sigma_t$ , and by criterion 2 (substitution invariance)  $\llbracket P' \rrbracket_{N'} \sigma_t \simeq \llbracket P' \sigma_s \rrbracket$ . As we know that  $P' \Downarrow u$ , this implies that  $P' \sigma_s \Downarrow \sigma_s(u)$ , which again implies that  $\llbracket P' \sigma_s \rrbracket_{N'} \Downarrow \sigma_t(\varphi(u))$ , which implies  $\llbracket P' \rrbracket_{N'} \sigma_t \Downarrow m$ . This establishes that

$$\llbracket P \rrbracket_N \sigma_t \rightarrow^* T' \sigma_t \wedge T' \sigma_t \simeq \llbracket P' \rrbracket_{N'} \sigma_t \wedge \llbracket P' \rrbracket_{N'} \sigma_t \Downarrow m$$

again, as expected. By requirement 2 in Definition 4, since  $\llbracket P' \rrbracket_{N'} \sigma_t \simeq T' \sigma_t$ , it must therefore also be the case that  $T' \sigma_t \Downarrow m$ , and hence that  $\llbracket P \rrbracket_N \sigma_t \Downarrow m$ .

However, consider now the effect of applying the substitution  $\llbracket P \rrbracket_N \sigma_t$ . By criterion 1 (compositionality), we have that

$$\llbracket P \rrbracket_N \sigma_t = C \sigma_t \mid \llbracket P_1 \rrbracket_{N_1} \sigma_t \mid \llbracket P_2 \rrbracket_{N_2} \sigma_t = C \mid \llbracket P_1 \rrbracket_{N_1} \sigma_t \mid \llbracket P_2 \rrbracket_{N_2} \sigma_t$$

where we can eliminate the substitution from  $C$ , since  $\varphi(u) \notin N \cup N_1 \cup N_2$ , as this immediately would violate criterion 6 (parameter independence); and as we know that  $u \notin \text{fn}(P)$ , we therefore also know that  $\varphi(u) \notin \text{fn}(C)$ , since  $C$  at most can contain a subset of the ( $\varphi$ -translated) free names of the process and the parameters. Thus the substitution has no effect on  $C$ .

Now consider the two subterms  $\llbracket P_1 \rrbracket_{N_1} \sigma_t$  and  $\llbracket P_2 \rrbracket_{N_2} \sigma_t$ . By criterion 2,  $\llbracket P_1 \rrbracket_{N_1} \sigma_t \simeq \llbracket P_1 \sigma_s \rrbracket_{N_1}$  and  $\llbracket P_2 \rrbracket_{N_2} \sigma_t \simeq \llbracket P_2 \sigma_s \rrbracket_{N_2}$ , but when we apply the substitution, we get that

$$P_1 \sigma_s = (a \langle \ulcorner x_1 \urcorner \mid \ulcorner x_2 \urcorner \rangle) \sigma_s = a \langle \ulcorner x_1 \urcorner \mid \ulcorner x_2 \urcorner \rangle = P_1 \quad P_2 \sigma_s = (a(n).n \langle \mathbf{0} \rangle) \sigma_s = a(n).n \langle \mathbf{0} \rangle = P_2$$

since obviously  $u \notin \text{fn}(P_1)$  and  $u \notin \text{fn}(P_2)$ , so the substitution has no effect on any of the subterms. Thus

$$C \mid \llbracket P_1 \sigma_s \rrbracket_{N_1} \mid \llbracket P_2 \sigma_s \rrbracket_{N_2} = C \mid \llbracket P_1 \rrbracket_{N_1} \mid \llbracket P_2 \rrbracket_{N_2}$$

and hence  $\llbracket P \sigma_s \rrbracket_N = \llbracket P \rrbracket_N$ . By criterion 2 (substitution invariance)  $\llbracket P \sigma_s \rrbracket_N \simeq \llbracket P \rrbracket_N \sigma_t$ , and thus we have that  $\llbracket P \rrbracket_N \sigma_t \simeq \llbracket P \rrbracket_N$ . This then yields the desired contradiction, since, as established above,  $\llbracket P \rrbracket_N \sigma_t \Downarrow m$  but  $\llbracket P \rrbracket_N \not\Downarrow m$ , whilst by requirement 2 of Definition 4 it must hold that  $\llbracket P \rrbracket_N \sigma_t \simeq \llbracket P \rrbracket_N \wedge \llbracket P \rrbracket_N \sigma_t \Downarrow m \implies \llbracket P \rrbracket_N \Downarrow m$ .  $\square$

The above proof exploits the reflective capability of the  $\rho$ -calculus to create new, *free* names at runtime, which are therefore also observable and substitutable. Thus, a substitution can affect the reduct of a process, without affecting the process itself, if the reduction step creates a new name. This cannot be mimicked in the  $\pi$ -calculus, where names have no structure and cannot be composed at runtime. Any new *free* name appearing at runtime can therefore only come from the translation parameters, since it cannot come from the source term; but this would then violate the criterion of parameter independence,

since we would then have to choose the parameters such that they correspond to the names that will be created at runtime.

This result does not directly depend on the higher-order characteristics of the  $\rho$ -calculus, and adding higher-order behaviour to the  $\pi$ -calculus would not suffice to enable it to encode the  $\rho$ -calculus. In [18], Sangiorgi gave an encoding of the Higher-Order  $\pi$ -calculus,  $\text{HO}\pi$ , in the  $\pi$ -calculus. His encoding also satisfies our criteria from Definition 3, and we therefore also have the following result:

**Corollary 1.** *There is no encoding of the  $\rho$ -calculus into  $\text{HO}\pi$  satisfying the criteria of Definition 3, when  $\simeq$  satisfies the requirement in Definition 4.*

Indeed, if such an encoding existed, we could compose it with the encoding of  $\text{HO}\pi$  into the  $\pi$ -calculus, to obtain an encoding of the  $\rho$ -calculus into the  $\pi$ -calculus, in contradiction of Theorem 1. This also indicates that the key feature of the  $\rho$ -calculus which cannot be represented in the  $\pi$ -calculus, is not its higher-order characteristics per se, but rather its capability for reflection, which gives it higher-order characteristics as a by-product.

## 8 Related works

The issues of encodability and assessing the relative expressiveness of various process calculi has been considered by several authors; in particular, Gorla [8] proposed a framework for reasoning about encodability and separation w.r.t. a set of criteria that also served as inspiration for the criteria used in the present paper. Towards the end of the paper, Gorla also discusses some of the difficulties involved in formulating a *general* framework for encodability in the presence of parameters, which particularly pertain to the question of which language the names belong to (the source or the target). In the present case, the answer is clearly the target language, which is further underscored by our restrictions on observability and compositionality; i.e. that the parameters should not be observable in the source term; and that, for each recursive call to the translation function, the parameters should be derivable from the initial set. Furthermore, we have added the criterion of parameter independence. We believe that such a criterion will generally be necessary for encodings that allow the set of parameters to ‘evolve’ or be updated in some structured way during the course of the translation, which seems particularly likely when we are working with structured names or terms. More recently, van Glabbeek [7] has also proposed a definition of a valid encoding, which he derives from a notion of a semantic equivalence or preorder, rather than basing it on a list of commonly agreed-upon criteria (as we have done in the present paper, following Gorla). However, this work also does not consider parametrised translations.

Also related is the work by Carbone and Maffeis [4] on expressivity of polyadic synchronisation. Their  ${}^e\pi$ -calculus substitutes names for names (as in the  $\pi$ -calculus), but allows  $n$ -ary vectors of names  $x_1 \cdot \dots \cdot x_n$  of arbitrary length  $n \geq 0$  to appear in *subject* position of input/output prefixes, and subjects must then match on all  $n$  names to yield a reduction. Thus name vectors can be altered at runtime, but they cannot grow in length as in the  $\rho$ -calculus. However, we could conceive of a (purposefully ill-sorted) variant of  ${}^e\pi$  that would allow entire vectors of names to be substituted for single names, thereby allowing new vectors of increasing length to be composed at runtime. We do not know if such a calculus could encode the  $\rho$ -calculus, but we suspect that it might, if equipped with an appropriate notion of name equivalence.

Another approach to using structured terms as names is given by Bengtson et al. [2, 3] and Parrow et al. [15] in their work on  $\Psi$ -calculi, which is based on the theory of nominal sets and datatypes by Gabbay and Pitts [6].  $\Psi$ -calculi allow both subjects and objects to be terms from an arbitrary nominal datatype,

and with substitution of terms for names. This enables runtime composition of terms, and, notably, the  $\rho$ -calculus *can* be instantiated as a (higher-order)  $\Psi$ -calculus, as the present author and others have shown in [1].

## 9 Conclusion

The original  $\rho$ -calculus paper [11] by Meredith and Radestock raises some interesting questions about the nature of names in process calculi. By including name generation in the language, it forces any process to give an explicit account of the source of any fresh names required during its execution, whilst this is entirely implicit in the  $\pi$ -calculus with the  $(\nu x)P$  operator. This adds a degree of realism to the  $\rho$ -calculus, which may be relevant from an implementation perspective, but also requires some extra care when we wish to reason about it formally. For example, Meredith and Radestock attempted to show that the  $\pi$ -calculus can be interpreted in the  $\rho$ -calculus, but their encoding did not properly account for the invariant that must hold for the names used as parameters in their encoding; i.e. that the parameters always refer to the most recently replicated names, leading to two errors that invalidate their correctness result. The purpose of the present paper has been to describe these errors and then give a new encoding of the  $\pi$ -calculus, for which we have shown correctness w.r.t. a set of criteria for encodability close to those proposed by Gorla [8]. The main difference is that we here use a parametrised translation, and we therefore had to take parameters into account in our criteria. This seems unavoidable when we are working with a calculus with structured names like the  $\rho$ -calculus, where all names are global and cannot be declared at runtime.

Our encoding works, modulo the criteria in Definition 3; yet it may not be an entirely satisfactory solution in at least one regard: the name server acts as a single, central source of fresh names. If we consider the scenarios one might wish to *model* in the  $\pi$ -calculus, having such a single central process might be acceptable for e.g. models of programs running on a single computer, or models of client-server systems with a star topology. However, for distributed systems with a different network topology, the translation would not yield an adequate representation. Thus, the encoding may preserve the semantics of a program, but not necessarily the intuitions underlying its structure. We could instead conceive of a more elaborate encoding, where e.g. each replication also instantiates its own copy of a name server to service the replicated processes. This would be closer to the intention in the encoding by Meredith and Radestock; but as we have seen, one would then have to be careful to ensure that each replica of the name server will generate a distinct namespace to avoid the possibility of a name clash. This could be achieved by letting each replica first request fresh names for all its parameters, including the namespace root  $s$  which must then be composed or otherwise shifted into a new namespace. Yet this creates a scaffolding problem, where, in order to instantiate a new source of fresh names, one must first have a source of fresh names. It does not remove the need for an initial, ‘top level’ instance of the name server. These considerations illustrate some of the difficulties involved in working with, and reasoning about, structured names with global visibility. None of these problems are present in the  $\pi$ -calculus, yet any implementation of a  $\pi$ -calculus program would need to include a solution to the problem of obtaining fresh names. In the words of Meredith and Radestock [11], the  $\pi$ -calculus does not provide a ‘theory of names.’

We have also shown that the  $\pi$ -calculus cannot encode the  $\rho$ -calculus in a way that satisfies the same criteria, modulo some requirements on the notion of behavioural equivalence  $\simeq$  used in Definition 4. The key to this separation result seems precisely to be the ability of the  $\rho$ -calculus to create new *free* names at runtime, which cannot be mimicked in the  $\pi$ -calculus. This ability is a consequence of *reflection* in the



$\rho$ -calculus, which also gives it higher-order characteristics as a by-product. In a process-calculus setting where computation is modelled as communication, higher-order behaviour appears as just a special case of reflection, where processes (code) are transmitted without modification. Thus, the separation result is also interesting in light of a remark by Sangiorgi regarding the encodability of  $\text{HO}\pi$  into the  $\pi$ -calculus. He notes that this “[...] *proves that the first-order paradigm, being by far simpler, should be taken as basic. Such a conclusion takes away the interest in the opposite direction, namely the representability of the  $\pi$ -calculus within a language using purely communications of agents ...*” [17, p. 8]. But as we have seen, this does not seem to hold in the more general case where higher-order characteristics derive from the capability of reflection. The  $\rho$ -calculus purely uses communication of agents (processes), because names and processes are the same thing.

## Acknowledgements

The author wishes to thank Hans Hüttel, Bjarke B. Bojesen and Alex R. Bendixen for many discussions of the  $\rho$ -calculus, and Luca Aceto and the anonymous reviewers for their numerous and invaluable comments on earlier drafts of this paper.

## References

- [1] Alex Rønning Bendixen, Bjarke Bredow Bojesen, Hans Hüttel & Stian Lybech (2022): *A Generic Type System for Higher-Order  $\Psi$ -calculi*. *Electronic Proceedings in Theoretical Computer Science* 368, Open Publishing Association, pp. 43–59, doi:10.4204/EPTCS.368.3.
- [2] Jesper Bengtson, Magnus Johansson, Joachim Parrow & Björn Victor (2009): *Psi-calculi: Mobile processes, nominal data, and logic*. In: *2009 24th Annual IEEE Symposium on Logic In Computer Science*, IEEE, pp. 39–48, doi:10.1016/S1571-0661(05)80361-5.
- [3] Jesper Bengtson, Magnus Johansson, Joachim Parrow & Björn Victor (2011): *Psi-calculi: a framework for mobile processes with nominal data and logic*. *Logical Methods in Computer Science* Volume 7, Issue 1, doi:10.2168/LMCS-7(1:11)2011. Available at <https://lmcs.episciences.org/696>.
- [4] Marco Carbone & Sergio Maffei (2003): *On the Expressive Power of Polyadic Synchronisation in Pi-Calculus*. *Nordic Journal of Computing* 10(2), pp. 70–98, doi:10.1016/S1571-0661(05)80361-5.
- [5] Cédric Fournet & Georges Gonthier (2000): *The Join Calculus: A Language for Distributed Mobile Programming*. In: *International Summer School on Applied Semantics*, Springer, pp. 268–332, doi:10.1007/3-540-45699-6\_6.
- [6] Murdoch Gabbay & Andrew Pitts (2002): *A New Approach to Abstract Syntax with Variable Binding*. *Formal Asp. Comput.* 13, pp. 341–363, doi:10.1007/s001650200016.
- [7] Rob van Glabbeek (2018): *A theory of encodings and expressiveness*. In: *International Conference on Foundations of Software Science and Computation Structures*, Springer, Cham, pp. 183–202, doi:10.1007/978-3-319-89366-2\_10.
- [8] Daniele Gorla (2010): *Towards a unified approach to encodability and separation results for process calculi*. *Information and Computation* 208(9), pp. 1031–1053, doi:10.1016/j.ic.2010.05.002.
- [9] Daniele Gorla & Uwe Nestmann (2014): *Full abstraction for expressiveness: history, myths and facts*. *Mathematical Structures in Computer Science* 26, pp. 639 – 654, doi:10.1017/S0960129514000279.
- [10] Stian Lybech (2022): *Encodability and Separation for a Reflective Higher-Order Calculus*. Technical Report, Department of Computer Science, Reykjavík University. Available at [http://icetcs.ru.is/stian/2022/reflection\\_encodability2022techreport.pdf](http://icetcs.ru.is/stian/2022/reflection_encodability2022techreport.pdf).

- [11] L.G. Meredith & Matthias Radestock (2005): *A Reflective Higher-order Calculus*. *Electronic Notes in Theoretical Computer Science* 141(5), pp. 49 – 67, doi:10.1016/j.entcs.2005.05.016. Proceedings of the Workshop on the Foundations of Interactive Computation (FInCo 2005).
- [12] Robin Milner (1993): *The Polyadic  $\pi$ -Calculus: a Tutorial*. In: *Logic and Algebra of Specification*, Springer Berlin Heidelberg, pp. 203–246, doi:10.1007/978-3-642-58041-3\_6.
- [13] Robin Milner, Joachim Parrow & David Walker (1992): *A calculus of mobile processes, I*. *Information and Computation* 100(1), pp. 1–40, doi:10.1016/0890-5401(92)90008-4.
- [14] Joachim Parrow (2001): *An introduction to the  $\pi$ -calculus*. In: *Handbook of Process Algebra*, Elsevier, pp. 479–543, doi:10.1016/B978-044482830-9/50026-6.
- [15] Joachim Parrow, Johannes Borgström, Palle Raabjerg & Johannes Åman Pohjola (2014): *Higher-order psi-calculi*. *Mathematical Structures in Computer Science* 24(2), doi:10.1017/S0960129513000170.
- [16] Benjamin C. Pierce & David N. Turner (2000): *Pict: a programming language based on the Pi-Calculus*. In: *Proof, Language, and Interaction*, pp. 455–494, doi:10.5555/345868.345924.
- [17] Davide Sangiorgi (1993): *Expressing mobility in process algebras: first-order and higher-order paradigms*. Ph.D. thesis, University of Edinburgh. Available at <http://hdl.handle.net/1842/6569>.
- [18] Davide Sangiorgi (1993): *From  $\pi$ -calculus to higher-order  $\pi$ -calculus — and back*. In M. C. Gaudel & J. P. Jouannaud, editors: *TAPSOFT'93: Theory and Practice of Software Development*, Springer Berlin Heidelberg, pp. 151–166, doi:10.1007/3-540-56610-4\_62.
- [19] Brian Cantwell Smith (1982): *Procedural Reflection in Programming Languages*. Ph.D. thesis, Massachusetts Institute of Technology. Available at <http://hdl.handle.net/1721.1/15961>.
- [20] David N. Turner (1996): *The Polymorphic Pi-calculus: Theory and Implementation*. Ph.D. thesis, University of Edinburgh, UK. Available at <https://hdl.handle.net/1842/395>.