A type system for a reflective higher-order calculus

L.G. MEREDITH AND MATTHIAS RADESTOCK

Abstract. The interplay between name construction and process construction allows pattern matching on names to constrain process behavior. Additionally, the notion of restriction is interrogated at a fundamental level.

1. Introduction

Blah, blah, blah...

1.1. **Overview and contributions.** We provide a type system for a reflective higher-order calculus. We propose a novel notion of hiding in which cryptographic capability is used to hide channels rather than the other way around.

2. The calculus

2.0.1. *Notation.* We let P, Q, R range over processes and x, y, z range over names.

ρ-calculus	P, Q	$::=$	0	null process
		$\mid$	$x(y)\,.\,P$	input
		$\mid$	$x\langle\!\lvert P \rvert\!\rangle$	lift
		$\mid$	$\ulcorner x \urcorner$	drop
		$\mid$	$P \mid Q$	parallel
	x, y	$::=$	$\lceil P \rceil$	quote

2.0.2. *Input and output.* The input constructor is standard for an asynchronous name-passing calculus. Input blocks its continuation from execution until it receives a communication. Lift is a form of output which – because the calculus is asynchronous – is allowed no continuation. It also affords a convenient syntactic sugar, which we define here.

$$x[y] \triangleq x\langle\!\lvert \ulcorner y \urcorner \rvert\!\rangle$$

Key words and phrases. concurrency, message-passing, process calculus, reflection.

2.1. **Free and bound names.** The syntax has been chosen so that a binding occurrence of a name is sandwiched between round braces, $(\cdot)$. Thus, the calculation of the free names of a process, P, denoted $\mathcal{FN}(P)$ is given recursively by

$$\begin{aligned}
\mathcal{FN}(0) &= \emptyset \\
\mathcal{FN}(x(y)\,.\,P) &= \{x\} \cup (\mathcal{FN}(P) \setminus \{y\}) \\
\mathcal{FN}(x\langle\!|P|\!\rangle) &= \{x\} \cup \mathcal{FN}(P) \\
\mathcal{FN}(P \mid Q) &= \mathcal{FN}(P) \cup \mathcal{FN}(Q) \\
\mathcal{FN}(\ulcorner x \urcorner) &= \{x\}
\end{aligned}$$

An occurrence of x in a process P is *bound* if it is not free. The set of names occurring in a process (bound or free) is denoted by $\mathcal{N}(P)$.

2.2. **Structural congruence.** The *structural congruence* of processes, noted $\equiv$, is the least congruence, containing α-equivalence, $\equiv_\alpha$, that satisfies the following laws:

$$\begin{aligned}
P \mid 0 &\equiv P \equiv 0 \mid P \\
P \mid Q &\equiv Q \mid P \\
(P \mid Q) \mid R &\equiv P \mid (Q \mid R)
\end{aligned}$$

2.3. **Name equivalence.** We now come to one of the first real subtleties of this calculus. Both the calculation of the free names of a process and the determination of structural congruence between processes critically depend on being able to establish whether two names are equal. In the case of the calculation of the free names of an input-guarded process, for example, to remove the bound name we must determine whether it is in the set of free names of the continuation. Likewise, structural congruence includes α-equivalence. But, establishing α-equivalence between the processes $x(z)\,.\,w\langle\!|y[z]|\!\rangle$ and $x(v)\,.\,w\langle\!|y[v]|\!\rangle$, for instance, requires calculating a substitution, e.g. $x(v)\,.\,w\langle\!|y[v]|\!\rangle\{z/v\}$. But this calculation requires, in turn, being able to determine whether two names, in this case the name in the object position of the output, and the name being substituted for, are equal.

As will be seen, the equality on names involves structural equivalence on processes, which in turn involves alpha equivalence, which involves name equivalence. This is a subtle mutual recursion, but one that turns out to be well-founded. Before presenting the technical details, the reader may note that the grammar above enforces a strict alternation between quotes and process constructors. Each question about a process that involves a question about names may in turn involve a question about processes, but the names in the processes the next level down, as it were, are under fewer quotes. To put it another way, each 'recursive call' to name equivalence will involve one less level of quoting, ultimately bottoming out in the quoted zero process.

Let us assume that we have an account of (syntactic) substitution and α-equivalence upon which we can rely to formulate a notion of name equivalence, and then bootstrap our notions of substitution and α-equivalence from that. We take name equivalence, written $\equiv_N$, to be the smallest equivalence relation generated by the following rules.

$$\frac{}{\ulcorner\urcorner x \ulcorner\urcorner \equiv_N x} \qquad \text{(Quote-drop)}$$

$$\frac{P \equiv Q}{\ulcorner P \urcorner \equiv_N \ulcorner Q \urcorner} \qquad \text{(STRUCT-EQUIV)}$$

2.4. **Syntactic substitution.** Now we build the substitution used by α-equivalence. We use $Proc$ for the set of processes, $\ulcorner Proc \urcorner$ for the set of names, and $\{\vec{y}/\vec{x}\}$ to denote partial maps, $s : \ulcorner Proc \urcorner \to \ulcorner Proc \urcorner$. A map, s lifts, uniquely, to a map on process terms, $\widehat{s} : Proc \to Proc$ by the following equations.

$$\begin{aligned}
(0)\{\widehat{\ulcorner Q \urcorner/\ulcorner P \urcorner}\} &= 0 \\
(R \mid S)\{\widehat{\ulcorner Q \urcorner/\ulcorner P \urcorner}\} &= (R)\{\widehat{\ulcorner Q \urcorner/\ulcorner P \urcorner}\} \mid (S)\{\widehat{\ulcorner Q \urcorner/\ulcorner P \urcorner}\} \\
(x(y)\,.\,R)\{\widehat{\ulcorner Q \urcorner/\ulcorner P \urcorner}\} &= (x)\{\ulcorner Q \urcorner/\ulcorner P \urcorner\}(z)\,.\,((R\{\widehat{z/y}\})\{\widehat{\ulcorner Q \urcorner/\ulcorner P \urcorner}\}) \\
(x\langle\!|R|\!\rangle)\{\widehat{\ulcorner Q \urcorner/\ulcorner P \urcorner}\} &= (x)\{\ulcorner Q \urcorner/\ulcorner P \urcorner\}\langle\!|R\{\widehat{\ulcorner Q \urcorner/\ulcorner P \urcorner}\}|\!\rangle \\
(\urcorner x \ulcorner)\{\widehat{\ulcorner Q \urcorner/\ulcorner P \urcorner}\} &= \begin{cases} \urcorner\ulcorner Q \urcorner\ulcorner & x \equiv_N \ulcorner P \urcorner \\ \urcorner x \ulcorner & otherwise \end{cases}
\end{aligned}$$

where

$$(x)\{\ulcorner Q \urcorner/\ulcorner P \urcorner\} = \begin{cases} \ulcorner Q \urcorner & x \equiv_N \ulcorner P \urcorner \\ x & otherwise \end{cases}$$

and z is chosen distinct from $\ulcorner P \urcorner$, $\ulcorner Q \urcorner$, the free names in Q, and all the names in R. Our α-equivalence will be built in the standard way from this substitution.

But, given these mutual recursions, the question is whether the calculation of $\equiv_N$ (respectively, $\equiv$, $\equiv_\alpha$) terminates. To answer this question it suffices to formalize our intuitions regarding level of quotes, or quote depth, $\#(x)$, of a name x as follows.

$$\begin{aligned}
\#(\ulcorner P \urcorner) &= 1 + \#(P) \\
\#(P) &= \begin{cases} max\{\#(x) : x \in \mathcal{N}(P)\} & \mathcal{N}(P) \neq \emptyset \\ 0 & otherwise \end{cases}
\end{aligned}$$

The grammar ensures that $\#(\ulcorner P \urcorner)$ is bounded. Then the termination of $\equiv_N$ (respectively, $\equiv$, $\equiv_\alpha$) is an easy induction on quote depth.

2.5. **Semantic substitution.** The substitution used in α-equivalence is really only a device to formally recognize that binding occurrences do not depend on the specific names. It is not the engine of computation. The proposal here is that while synchronization is the driver of that engine, the real engine of computation is a semantic notion of substitution that recognizes that a dropped name is a request to run a process. Which process? Why the one whose code has been bound to the name being dropped. Formally, this amounts to a notion of substitution that differs from syntactic substitution in its application to a dropped name.

$$(\urcorner x \ulcorner)\{\widehat{\ulcorner Q \urcorner/\ulcorner P \urcorner}\} = \begin{cases} Q & x \equiv_N \ulcorner P \urcorner \\ \urcorner x \ulcorner & otherwise \end{cases}$$

In the remainder of the paper we will refer to semantic and syntactic substitutions simply as substitutions and rely on context to distinguish which is meant. Similarly, we will abuse notation and write $\{y/x\}$ for $\widehat{\{y/x\}}$.

Finally equipped with these standard features we can present the dynamics of the calculus.

2.6. **Operational Semantics.** The reduction rules for ρ-calculus are

$$\frac{x_0 \equiv_N x_1}{x_0(\!|Q|\!) \mid x_1(y)\,.\,P \to P\{\ulcorner Q \urcorner/y\}} \quad \text{(Comm)}$$

In addition, we have the following context rules:

$$\frac{P \to P'}{P \mid Q \to P' \mid Q} \quad \text{(Par)}$$

$$\frac{P \equiv P' \qquad P' \to Q' \qquad Q' \equiv Q}{P \to Q} \quad \text{(Equiv)}$$

The context rules are entirely standard and we do not say much about them, here. The communication rule does what was promised, namely make it possible for agents to synchronize and communicate processes packaged as names. But, it also provides a scheme that identifies the role of name equality in synchronization. There are other relationships between names with structure that could also mediate synchronization. Consider, for example, a calculus identical to the one presented above, but with an alternative rule governing communication.

$$\frac{\forall R.[P_{channel} \mid Q_{channel} \to^* R] \Rightarrow R \to^* 0}{\ulcorner Q_{channel} \urcorner(\!|Q|\!) \mid \ulcorner P_{channel} \urcorner(y)\,.\,P \to P\{\ulcorner Q \urcorner/y\}} \quad \text{(Comm-annihilation)}$$

Intuitively, it says that the codes of a pair of processes, $P_{channel}$, $Q_{channel}$, stand in channel/co-channel relation just when the composition of the processes always eventually reduces to 0, that is, when the processes annihilate one another. This rule is well-founded, for observe that because $0 \equiv 0 \mid 0$, $0 \mid 0 \to^* 0$. Thus, $\ulcorner 0 \urcorner$ serves as its own co-channel. Analogous to our generation of names from 0, with one such channel/co-channel pair, we can find many such pairs. What we wish to point out about this rule is that we can see precisely an account of the calculation of the channel/co-channel relationship as deriving from the theory of interaction. We do not know if the computation of name equality has a similar presentation, driving home the potential difference of those two roles in calculi of interaction.

There is no reason why 0 is special in the scheme above. We observe a family of calculi, indexed by a set of processes $\{S_\alpha\}$, and differing only in their communication rule each of which conforms to the scheme below.

$$\frac{\forall R.[P_{channel} \mid Q_{channel} \to^* R] \Rightarrow R \to^* R' \equiv S_\alpha}{\ulcorner Q_{channel} \urcorner(\!|Q|\!) \mid \ulcorner P_{channel} \urcorner(y)\,.\,P \to P\{\ulcorner Q \urcorner/y\}} \quad \text{(Comm-annihilation-S)}$$

Given this discussion, we write $x \div y$ when x and y stand in channel/co-channel relation. In the first system presented, $x \div y \Leftrightarrow x \equiv_N y$, while in the system with the comm-annihilation rule, $\ulcorner P \urcorner \div \ulcorner Q \urcorner \Leftrightarrow \forall R.[P \mid Q \to^* R] \Rightarrow R \to^* 0$.

3. Replication

As mentioned before, it is known that replication (and hence recursion) can be implemented in a higher-order process algebra [**?**]. As our first example of calculation with the machinery thus far presented we give the construction explicitly in the ρ-calculus.

$$\begin{array}{rcl} D(x) & \triangleq & x(y) \,.\, (x[y] \mid \ulcorner y \urcorner) \\ !P(x) & \triangleq & x(\!| D(x) \mid P |\!) \mid D(x) \end{array}$$

Of course, this encoding, as an implementation, runs away, unfolding $!P$ eagerly. A lazier and more implementable replication operator, restricted to input-guarded processes, may be obtained as follows.

$$!u(v) \,.\, P \triangleq x(\!| u(v) \,.\, (D(x) \mid P) |\!) \mid D(x)$$

4. Bisimulation

Having taken the notion of restriction out of the language, we carefully place it back into the notion of observation, and hence into the notion of program equality, i.e. bisimulation. That is, we parameterize the notion of barbed bisimulation by a set of names over which we are allowed to set the barbs. The motivation for this choice is really comparison with other calculi. The set of names of the ρ-calculus is *global*. It is impossible, in the grammar of processes, to guard terms from being placed into contexts that can potentially observe communication. So, we provide a place for reasoning about such limitations on the scope of observation in the theory of bisimulation.

Definition 4.0.1. An *observation relation*, $\downarrow_{\mathcal{N}}$, over a set of names, $\mathcal{N}$, is the smallest relation satisfying the rules below.

$$\frac{y \in \mathcal{N},\ x \equiv_N y}{x[v] \downarrow_{\mathcal{N}} x} \qquad \text{(Out-barb)}$$

$$\frac{P \downarrow_{\mathcal{N}} x \text{ or } Q \downarrow_{\mathcal{N}} x}{P \mid Q \downarrow_{\mathcal{N}} x} \qquad \text{(Par-barb)}$$

We write $P \Downarrow_{\mathcal{N}} x$ if there is Q such that $P \Rightarrow Q$ and $Q \downarrow_{\mathcal{N}} x$.

Notice that $x(y) \,.\, P$ has no barb. Indeed, in ρ-calculus as well as other asynchronous calculi, an observer has no direct means to detect if a message sent has been received or not.

Definition 4.0.2. An $\mathcal{N}$-*barbed bisimulation* over a set of names, $\mathcal{N}$, is a symmetric binary relation $\mathcal{S}_{\mathcal{N}}$ between agents such that $P \,\mathcal{S}_{\mathcal{N}}\, Q$ implies:

(1) If $P \to P'$ then $Q \Rightarrow Q'$ and $P' \,\mathcal{S}_{\mathcal{N}}\, Q'$.
(2) If $P \downarrow_{\mathcal{N}} x$, then $Q \Downarrow_{\mathcal{N}} x$.

P is $\mathcal{N}$-barbed bisimilar to Q, written $P \dot{\approx}_{\mathcal{N}} Q$, if $P \,\mathcal{S}_{\mathcal{N}}\, Q$ for some $\mathcal{N}$-barbed bisimulation $\mathcal{S}_{\mathcal{N}}$.

5. Type system

ρ-calculus-types	T, U	$::=$	0	null process
		$\mid$	$t[u]$	output
		$\mid$	$t(u)\,.\,T$	input
		$\mid$	$\ulcorner v \urcorner$	drop
		$\mid$	$T \mid U$	parallel
	t, u	$::=$	v	variable
		$\mid$	$\ulcorner T \urcorner$	quote

5.0.1. *Notation.* We need to be able to strip quotes from entities in the syntactic category ranged over by t and u in the grammar above. Any such entity will be either a variable, v, or a quoted type, T. We overload the drop notation.

$$\begin{aligned} \ulcorner v \urcorner &= v \\ \ulcorner \ulcorner T \urcorner \urcorner &= T \end{aligned}$$

5.1. **Pattern-matching on names.**

Definition 5.1.1 (pattern substitution)**.** A *pattern substitution* is a partial map from variables to names. We let ϱ, σ range over pattern substitutions. When context allows no ambiguity we refer to a pattern substitution simply as a substitution. Finite substitutions will be written $\{v \mapsto \ulcorner P \urcorner, ...\}$. We write $\varrho : \sigma$ for the extension of ϱ by σ. Two substitutions, ϱ, σ, are *compatible*, written $\varrho \sim \sigma$, if and only if $\forall v \in Dom(\varrho) \cap Dom(\sigma).\varrho(v) = \sigma(v)$.

Substitutions lift to maps from types to types in the usual way. The application of a substitution, ϱ, to a type, T, is written $T\varrho$. A type, T, is *ground* if it has no occurrences of a variable in it. We write $\mathcal{G}(T)$ to assert that T is ground. Given two types, T and U, we say they are *compatible*, $T \asymp W$, if and only if $\exists \varrho.\mathcal{G}(T\varrho)\&\mathcal{G}(U\varrho)\&T\varrho \doteqdot U\varrho$.

5.2. **Hiding and cryptography.** The connection between the restriction operator and secrecy has long been noted [**?**] [**?**]. Here, we revisit this notion in the light of names with structure. We posit names and co-names as key pairs. Then, we propose a family of functions, $\{\mathcal{H}\}$, an element of which

- takes a pair of names (respectively quoted patterns) and a process (repectively type);
- produces two new names (respectively quoted patterns) that are the encryptions of the ones supplied;
- replaces the originals with the encrypted versions in the process (respectively type).

The encryption scheme, write it $\mathcal{H}_{\mathcal{E}}$, of each $\mathcal{H}$ is required to satisfy the condition

$$x \doteqdot y \Rightarrow \mathcal{H}_{\mathcal{E}}(x, y)(x) \doteqdot \mathcal{H}_{\mathcal{E}}(x, y)(y)$$

That is, if x and y are in channel/co-channel relation, then their encrypted versions also stand in channel/co-channel relation. Note: this will not actually hide all communications on the channels. An eaves-dropper could get lucky. It depends on the strength of the encryption.

Example 5.2.1. Let $T \triangleq v_0[\![v_1]\!] \mid v_1(\!(v_0)\!).\ulcorner v_2 \urcorner$, and $\mathcal{H}_{\mathcal{E}}(x,y)(z) \triangleq T\{x/v_0\}\{y/v_1\}\{z/v_2\}$. Then, if $x \doteqdot y \Leftrightarrow x \equiv_N y$, then $\mathcal{H}_{\mathcal{E}}$ satisfies the condition.

$$\frac{}{\varepsilon, \ulcorner 0 \urcorner \vdash \ulcorner 0 \urcorner} \quad \text{(NULL)}$$

$$\frac{}{\{v \mapsto \ulcorner P \urcorner\}, \ulcorner P \urcorner \vdash v} \quad \text{(VARIABLE)}$$

$$\frac{\varrho, \ulcorner P \urcorner \vdash t, \qquad \sigma, \ulcorner Q \urcorner \vdash u, \qquad \varrho \sim \sigma}{\varrho : \sigma, \ulcorner\ulcorner P \urcorner \langle\!| Q |\!\rangle \urcorner \vdash \ulcorner t[\![u]\!] \urcorner} \quad \text{(LIFT)}$$

$$\frac{\varrho, \ulcorner P \urcorner \vdash t, \qquad \sigma, \ulcorner Q \urcorner \vdash u, \qquad \varrho \sim \sigma}{\varrho : \sigma, \ulcorner\ulcorner P \urcorner(\!(x)\!) \,.\, Q \urcorner \vdash \ulcorner t(\!(v)\!) \,.\, u \urcorner} \quad \text{(INPUT)}$$

$$\frac{\varrho, \ulcorner P \urcorner \vdash t, \qquad \sigma, \ulcorner Q \urcorner \vdash u, \qquad \varrho \sim \sigma}{\varrho : \sigma, \ulcorner P \mid Q \urcorner \vdash \ulcorner\ulcorner t \urcorner \mid \ulcorner u \urcorner\urcorner} \quad \text{(PARALLEL)}$$

5.3. **Type judgment.** Now, for the type judgment rules. These rules are really a scheme, instantiated by a given cryptographic function, $\mathcal{H}$.

$$\frac{}{0 : 0} \quad \text{(NULL)}$$

$$\frac{}{\ulcorner x \urcorner : \ulcorner v \urcorner} \quad \text{(DROP)}$$

$$\frac{\varrho, \ulcorner P \urcorner \vdash t, \qquad Q : U}{\ulcorner P \urcorner \langle\!| Q |\!\rangle : t[\![\ulcorner U \urcorner]\!]} \quad \text{(LIFT)}$$

$$\frac{\varrho, \ulcorner P \urcorner \vdash t, \qquad Q : U}{\ulcorner P \urcorner(\!(x)\!) \,.\, Q : t(\!(v)\!) \,.\, U} \quad \text{(INPUT)}$$

$$\frac{x_0 \langle\!| R |\!\rangle \mid P : t[\![u]\!] \mid T, \qquad x_1(\!(y)\!) \,.\, Q : w(\!(v)\!) \,.\, U, \qquad \ulcorner t \urcorner \asymp \ulcorner w \urcorner}{\mathcal{H}(x_0, x_1)(x_0 \langle\!| R |\!\rangle \mid P \mid w(\!(v)\!) \,.\, U) : \mathcal{H}(t,w)(T \mid U\{u/v\})} \quad \text{(COMM)}$$

$$\frac{P : \ulcorner v \urcorner, \qquad Q : U}{P \mid Q : \ulcorner v \urcorner \mid U} \quad \text{(IND)}$$

Example 5.3.1. As our first example we type replication.

6. Conclusions and future work

Blah, blah, blah, types, blah...

Acknowledgments. The authors wish to acknowledge sleeplessness and chocolate.