The Reduction of Channels is Well-Behaved

Rodolphe Lepigre - LAMA, UMR 5127

13/10/2014

Language and Type System

We consider the classical extension of the simply-typed λ-calculus with the control opperator *call/cc* (denoted $\mathfrak{cc}$). The language is enriched with a new kind of terms, called channels, which are to be considered as typed constants for now.

$$t\,,\,u\,,\,v ::= x \mid \lambda x.t \mid (u)\,v \mid \mathfrak{cc} \mid [\alpha : \Delta \Rightarrow A] \qquad x \in \Lambda_x\,,\, \alpha \in \Lambda_\alpha$$

We denote $\Lambda_x = \{x\,,\,y\,,\,z\,...\}$ the set of λ-variables, and $\Lambda_\alpha = \{\alpha\,,\,\beta\,,\,\gamma...\}$ the set of channel names. These sets are supposed disjoint, and countable.

Definition 1. A channel is a term $[\alpha : \Delta \Rightarrow A]$ where $\alpha \in \Lambda_\alpha$ is a unique channel name, Δ is a context and A is a type.

We recall that a context is a finite set of type declarations of the form $x : A$, meaning that variable x is assumed to have type A. Contexts are usually ranged over by the letter Γ or Δ. Types are built from a countable set of atomic types (or base types) $\mathscr{B} = \{N\,,\,O\,,\,P...\}$, and from a countable set of type variables $\mathscr{V} = \{X, Y, Z...\}$, using the function arrow.

$$A\,,\,B\,,\,C ::= N \mid X \mid A \to B \qquad N \in \mathscr{B}, X \in \mathscr{V}$$

We will sometimes use the notation $\mathscr{P}_{A,B}$ for the formula $((A \to B) \to A) \to A$ (Peirce's Law). It will be used, in particular, to type the constant $\mathfrak{cc}$, and thus allow us to recover the full power of classical logic.

A typing judgement is of the form $\Gamma \vdash t : A$, where Γ is a context, t is a term and A is a type. When $\Gamma = \emptyset$ we will write $\vdash t : A$, and when $\Gamma = \Delta \uplus \{x : B\}$ we will sometimes write $\Delta, x : B \vdash t : A$. The full type-system of our language is exhibited bellow:

$$\frac{}{\Gamma, x : A \vdash x : A}\text{Ax} \qquad \frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x.t : A \to B}\to_i \qquad \frac{\Gamma \vdash u : A \to B \quad \Gamma \vdash v : A}{\Gamma \vdash (u)\,v : B}\to_e$$

$$\frac{}{\Gamma \vdash \mathrm{cc} : \mathscr{P}_{A,B}}\text{cc} \qquad \frac{\Delta \subseteq \Gamma}{\Gamma \vdash [\alpha : \Delta \Rightarrow A] : A}\text{Ch}$$

Note that the typing rule for channels has the form of an axiom (i.e. it does not have any premise), which makes it similar to a typing rule for a constant. However it requires for the context of the channel to be contained in the global context. The reason for this will come clear in the next section.

Closures, Stacks and Processes

We are going to work on closures, and not on terms, in order to keep the environment explicit. This will be absolutely necessary when we later decide to give a reduction rule to channels. Intuitively, a channel $[\alpha : \Delta \Rightarrow A]$ in head position is to be replaced by a term t such that $\Delta \vdash t : A$. In particular, such a term t might contain variables from Δ, and the environment is to provide a value to all these variables. If the environment is not kept explicit, the information about the reduced β-redexes will have disapeared, and the environment will know nothing about these variables.

We recall that a closure is a couple $\langle t, \sigma\rangle$ of a term t and an environment σ maping every free variable in t to a closure. We will use the notation $\sigma + \{x \mapsto c\}$ either to extend an environment by mapping (or re-mapping) variable x to the closure c, or to make explicit the fact that the considered environment is mapping variable x to the closure c. We give two typing rules allowing the construction of environments, and a typing rule allowing the construction of closures:

$$\frac{}{\vdash \emptyset : \emptyset}\sigma_\emptyset \qquad \frac{\vdash \sigma : \Gamma \quad \vdash c : A}{\vdash \sigma + \{x \mapsto c\} : \Gamma, x : A}\sigma_+$$

$$\frac{\vdash \sigma : \Gamma \quad \Gamma \vdash t : A}{\vdash \langle t, \sigma\rangle : A}<>_i$$

The first rule gives the empty context as a type for the empty environment, and the second rule extends an environment with a new closure mapping a new variable. The third rule builds a closure using an environment and a typing judgement for a term, provided that the type of the environment serves as the context for the typing of the term.

Since we are going to work in the settings of classical realizability, we need to define another kind of object: stacks, which are lists of closures. If π is a stack, and c is a closure, then $c.\pi$ is the stack built by pushing c on top of the stack π. We use the letter ε to denote the empty stack. The following two rules give a type to stacks:

$$\frac{}{\vdash \varepsilon : N^{\perp}}\,\varepsilon \qquad\qquad \frac{\vdash c : A \quad \vdash \pi : B^{\perp}}{\vdash c.\pi : (A \to B)^{\perp}}\,\pi$$

The first rule gives the type $N^{\perp}$ to the empty stack ε for an atomic type $N \in \mathscr{B}$. The second rule builds a stack by pushing a closure of type A on top of a stack of type $B^{\perp}$, resulting into a stack of type $(A \to B)^{\perp}$.

Note that a stack is a closed object, it does not contain any free variable. In fact, a stack can be considered as a constant, hence we associate a closure k_{π} to every stack π. The following rule gives the type $A \to B$ (for some type B) to the closure k_{π}, provided that π has type $A^{\perp}$.

$$\frac{\vdash \pi : A^{\perp}}{\vdash k_{\pi} : A \to B}\,k_{\pi}$$

We last need to define processes. A process is a couple of a closure c and of a stack π. It will be denoted $c \star \pi$, and will be used to represent the state of Krivine's Abstract Machine. Processes will be typed using the following rule:

$$\frac{\vdash c : A \quad \vdash \pi : A^{\perp}}{\vdash c \star \pi : \perp}\,\star$$

As a summary, we exhibit bellow the mutually recursive grammars generating the set of closures Λ and the set of stacks Π, and the grammar generating the set of processes $\Lambda \star \Pi$.

$$c ::= \langle t\,,\,\sigma\rangle \mid k_{\pi} \qquad \pi, \rho ::= c.\pi \mid \varepsilon \qquad p, q ::= c \star \pi$$

Reduction Rules, Realizability and Adequation Lemma

In this section we are going to give the classical realizability interpretation of our type-system. We first need to give the operational semantics of our language in terms of the reduction relation of Krivine's Abstract Machine. The one-step evaluation relation $>$ over the set of processes is defined by three rules allowing the machine to perform β-reduction, and two rule handling the classical part of computation.

$$\langle x\,,\,\sigma + \{x \mapsto c\}\rangle \star \pi \succ c \star \pi$$

$$\langle \lambda x.t\,,\,\sigma\rangle \star c.\pi \succ \langle t\,,\,\sigma + \{x \mapsto c\}\rangle \star \pi$$

$$\langle (t)\,u\,,\,\sigma\rangle \star \pi \succ \langle t\,,\,\sigma\rangle \star \langle u\,,\,\sigma\rangle.\pi$$

$$\langle \mathfrak{cc}\,,\,\sigma\rangle \star c.\pi \succ c \star k_\pi.\pi$$

$$k_\pi \star c.\pi' \succ c \star \pi$$

The classical realizability interpretation is parametrized by a pole $\perp\!\!\!\perp \subseteq \Lambda \star \Pi$, which is a set of processes closed under anti-evaluation. More formally, if $\perp\!\!\!\perp$ is a pole such that $p \in \perp\!\!\!\perp$ and if $q \succ p$, then $q \in \perp\!\!\!\perp$.

We call a valuation any function θ such that $\mathrm{dom}(\theta) \subseteq \mathscr{V}$, and for every type variable $X \in \mathrm{dom}(\theta)$, $\theta(X) \subseteq \Pi$. A parametric formula (resp. context) is simply a formula A (resp. context Γ) to which a valuation θ has been attached. This is denoted $A[\theta]$ (resp. $\Gamma[\theta]$). We say that a parametric formula A (resp. context Γ) is closed when every free type variable in A (resp. Γ) is in $\mathrm{dom}(\theta)$. Note that until second-order quantification is added to the language, every type variable appears free. We denote $\theta, X := S$ the extension of the valuation θ by mapping variable $X \notin \mathrm{dom}(\theta)$ to $S \subseteq \Pi$.

In order to be able to interpret base types, a function I associating every base type N to a set $\{\varepsilon\} \subseteq I_N \subseteq \Pi$ is to be provided. We now interpret every closed parametric formula $A[\theta]$ as a falsity value $\|A[\theta]\| \subseteq \Pi$ and a truth value $|A[\theta]| \subseteq \Lambda$ defined by mutual induction. We will sometimes write $|A[\theta]|_{\perp\!\!\!\perp}$ and $\|A[\theta]\|_{\perp\!\!\!\perp}$ in order to keep explicit the dependency with respect to a specific pole $\perp\!\!\!\perp$.

$$\|(A \to B)[\theta]\| = |A[\theta]|.\|B[\theta]\| = \{c.\pi \mid c \in |A[\theta]|\,,\, \pi \in \|B[\theta]\|\}$$

$$\|X[\theta]\| = \theta(X) \qquad\qquad \|N[\theta]\| = I_N$$

$$|A[\theta]| = \|A[\theta]\|^{\perp\!\!\!\perp} = \{c \in \Lambda \mid \forall \pi \in \|A[\theta]\|\;\; c \star \pi \in \perp\!\!\!\perp\}$$

Given a pole $\perp\!\!\!\perp$, we say that a closure $\langle t\,,\,\sigma\rangle$ realizes the closed parametric formula $A[\theta]$, denoted $\langle t, \sigma\rangle \Vdash_{\perp\!\!\!\perp} A[\theta]$, when $\langle t\,,\,\sigma\rangle \in |A[\theta]|$. We say that a substitution σ realizes the closed parametric context $\Gamma[\theta]$, written $\sigma \Vdash_{\perp\!\!\!\perp} \Gamma[\theta]$, when for every $x : A \in \Gamma$ we have $\sigma(x) \Vdash_{\perp\!\!\!\perp} A[\theta]$.

In order to state a theorem expressing the soundness of the realizability interpretation with respect to the type system, we need to provide a way to substitute channels with terms realizing their types. This is done using a channel substitution.

Definition 2. We denote $\mathrm{Chan}(\Psi)$ the set of channels contained in the term, environment, closure, stack or process Ψ. It is defined by induction on the structure of Ψ in a straight-forward way.

Definition 3. Let $⫫$ be a fixed pole, ψ be a term, an environment, a closure, a stack or a process with $\mathrm{chan}(\psi) = \{[\alpha_k : \Delta_k \Rightarrow A_k]\}_{k \in K}$ for some finite family of indices K. Let θ be a valuation such that for all $k \in K$, $\Delta_k[\theta]$ is a closed parametric context and $A_k[\theta]$ is a closed parametric formula. A channel assignment over Ψ is a substitution $\Sigma = \{\alpha_k \mapsto u_k\}_{k \in K}$ such that for every k and for every σ_k such that $\sigma_k \Vdash_{⫫} \Delta_k[\theta]$ we have $\langle u_k\,,\, \sigma_k\rangle \Vdash_{⫫} A_k[\theta]$. We denote $\Psi\Sigma$ the application of the channel assignment Σ on Ψ. This operation is defined by induction on the structure of Ψ in a straight-forward way.

Theorem 1. Let $⫫$ be a fixed pole, Σ be a channel assignment for a term t, σ be an environment, and θ be a valuation such that $\Gamma[\theta]$ is a closed parametric context and $A[\theta]$ is a closed parametric formula. If the judgement $\Gamma \vdash t : A$ is provable and if $\sigma \Vdash_{⫫} \Gamma[\theta]$, then $\langle t\Sigma\,,\, \sigma\rangle \Vdash_{⫫} A[\theta]$.

Proof. We do a proof by induction on the length of the proof of $\Gamma \vdash t : A$. We consider the rule used in the last step of the proof.

- Ax: we have $t = x$ and we must show that $\langle x\Sigma\,,\, \sigma\rangle \Vdash_{⫫} A[\theta]$, which is equivalent to showing that $\langle x\,,\, \sigma\rangle \star \pi \in ⫫$ for every stack $\pi \in \|A[\theta]\|$. By hypothesis we know that $\sigma \Vdash_{⫫} \Gamma[\theta]$, which gives us $\sigma(x) \star \pi \in ⫫$ for every stack $\pi \in \|A[\theta]\|$. We also know that $\langle x\,,\, \sigma\rangle \star \pi \succ \sigma(x) \star \pi$. Therefore, since $⫫$ is closed under anti-evaluation, we have $\langle x\,,\, \sigma\rangle \star \pi \in ⫫$ for every stack $\pi \in \|A[\theta]\|$.
- $\to_e$: we have $t = (u)\,v$ and we know that $\Gamma \vdash u : A \to B$ and $\Gamma \vdash v : A$. We must show that $\langle ((u)\,v)\Sigma\,,\, \sigma\rangle \Vdash_{⫫} B[\theta]$, which is equivalent to showing that $\langle (u\Sigma)\,v\Sigma\,,\, \sigma\rangle \star \pi \in ⫫$ for every stack $\pi \in \|B[\theta]\|$. By induction hypothesis we have $\langle u\Sigma\,,\, \sigma\rangle \Vdash_{⫫} (A \to B)[\theta]$ and $\langle v\Sigma\,,\, \sigma\rangle \Vdash_{⫫} A[\theta]$, which are equivalent by definition to $\langle u\Sigma\,,\, \sigma\rangle \in |(A \to B)[\theta]|$ and $\langle v\Sigma\,,\, \sigma\rangle \in |A[\theta]|$. Moreover $\langle v\Sigma\,,\, \sigma\rangle.\pi \in \|(A \to B)[\theta]\|$ for all $\pi \in \|B[\theta]\|$. This gives us $\langle u\Sigma\,,\, \sigma\rangle \star \langle v\Sigma\,,\, \sigma\rangle.\pi \in ⫫$ for every stack $\pi \in \|B[\theta]\|$. We also have $\langle (u\Sigma)\,v\Sigma\,,\, \sigma\rangle \star \pi \succ \langle u\Sigma\,,\, \sigma\rangle \star \langle v\Sigma\,,\, \sigma\rangle.\pi$, hence, since $⫫$ is closed under anti-evaluation we obtain that $\langle (u\Sigma)\,v\Sigma\,,\, \sigma\rangle \star \pi \in ⫫$ for every stack $\pi \in \|B[\theta]\|$.
- $\to_i$: we have $t = \lambda x.v$ and $\Gamma, x : A \vdash v : B$. We must show that $\langle (\lambda x.v)\Sigma\,,\, \sigma\rangle \Vdash_{⫫} (A \to B)[\theta]$, which is equivalent to showing that $\langle \lambda x.v\Sigma\,,\, \sigma\rangle \star \pi \in ⫫$ for every stack $\pi \in \|(A \to B)[\theta]\|$. By definition such stack has the form $c\,.\,\rho$ with $c \in |A[\theta]|$ and $\rho \in$

$\|B[\theta]\|$. By induction hypothesis we have $\langle \nu\Sigma\,,\, \sigma + \{x \mapsto c\}\rangle \Vdash_{\perp\!\!\!\perp} B[\theta]$, which means that $\langle \nu\Sigma\,,\, \sigma + \{x \mapsto c\}\rangle \star \rho \in \perp\!\!\!\perp$ for every stack $\rho \in \|B[\theta]\|$. Hence, since $\langle \lambda x.\nu\Sigma\,,\, \sigma\rangle \star c.\rho \succ \langle \nu\Sigma\,,\, \sigma + \{x \mapsto c\}\rangle \star \rho$ and $\perp\!\!\!\perp$ is closed under anti-evaluation we obtain that $\langle \lambda x.\nu\Sigma\,,\, \sigma\rangle \star c.\rho \in \perp\!\!\!\perp$ for every stack $\pi = c.\rho \in \|(A \to B)[\theta]\|$.

- $\mathfrak{cc}$: we have $t = \mathfrak{cc}$ and we must show that $\langle \mathfrak{cc}\Sigma\,,\, \sigma\rangle \Vdash_{\perp\!\!\!\perp} (((A \to B) \to A) \to A)[\theta]$ which is equivalent to showing that $\langle \mathfrak{cc}, \sigma\rangle \star \rho \in \perp\!\!\!\perp$ for every stack $\rho \in \|(((A \to B) \to A) \to B)[\theta]\|$. By definition, any such stack will have the form $c.\pi$, with $c \in |((A \to B) \to A)[\theta]|$ and $\pi \in \|A[\theta]\|$. Since we know that $\langle \mathfrak{cc}, \sigma\rangle \star c.\pi \succ c \star k_\pi.\pi$, it is enough to show that $c \star k_\pi.\pi \in \perp\!\!\!\perp$ for every $\pi \in \|A[\theta]\|$ and $c \in |((A \to B) \to A)[\theta]|$. To do so, it is enough to show that $k_\pi \in |(A \to B)[\theta]|$ for all $\pi \in \|A[\theta]\|$, which is equivalent to showing that $k_\pi \star \rho' \in \perp\!\!\!\perp$ for every stack $\rho' \in \|(A \to B)[\theta]\|$. But every such stack has the form $c'.\pi'$ with $c' \in |A[\theta]|$ and $\pi' \in \|B[\theta]\|$, and $k_\pi \star c'.\pi' \succ c' \star \pi$, hence it is enough to show that $c' \star \pi \in \perp\!\!\!\perp$, which is true since $c' \in |A[\theta]|$ and $\pi \in \|A[\theta]\|$.
- Ch: We consider $t = [\alpha : \Delta \Rightarrow A]$. We have $\Delta \subseteq \Gamma$, and we must show that $\langle [\alpha : \Delta \Rightarrow A]\Sigma\,,\, \sigma\rangle \Vdash_{\perp\!\!\!\perp} A[\theta]$. By hypothesis we know that $\langle [\alpha : \Delta \Rightarrow A]\Sigma\,,\, \sigma\rangle$ is equal to $\langle u\,,\, \sigma\rangle$ for some term u, and that $\sigma \Vdash_{\perp\!\!\!\perp} \Delta[\theta]$ (since $\Delta \subseteq \Gamma$). This gives us $\langle u\,,\, \sigma\rangle \Vdash_{\perp\!\!\!\perp} A[\theta]$. □

Theorem 2. Let $\perp\!\!\!\perp$ be a fixed pole, Σ be a channel assignment, and θ be a valuation such that $A[\theta]$ is a closed parametric formula and $\Gamma[\theta]$ is a closed parametric context.

1. If $\vdash c : A$ is provable, then $c\Sigma \Vdash_{\perp\!\!\!\perp} A[\theta]$.
2. If $\vdash \sigma : \Gamma$ is provable, then $\sigma\Sigma \Vdash_{\perp\!\!\!\perp} \Gamma[\theta]$.
3. If $\vdash \pi : A^\perp$ is provable, then $\pi\Sigma \in \|A[\theta]\|_{\perp\!\!\!\perp}$.

Proof. We do a proof by mutual induction. We consider the last rule used in the derivation of $\vdash c : A$, $\vdash \sigma : \Gamma$ or $\vdash \pi : A^\perp$:

- $\sigma_\emptyset$: since $\Gamma = \emptyset$ and $\sigma = \emptyset$, we trivially get $\sigma \Vdash_{\perp\!\!\!\perp} \Gamma[\theta]$.
- σ_+: we have a derivation of $\vdash \sigma : \Gamma$ and a derivation of $\vdash c : A$, and we must show that $(\sigma + \{x \mapsto c\})\Sigma \Vdash_{\perp\!\!\!\perp} (\Gamma, x : A)[\theta]$. By definition, this amounts to showing that for every $y : B$ in $\Gamma, x : T$ we have $(\sigma\Sigma + \{x \mapsto c\Sigma\})(y) \Vdash_{\perp\!\!\!\perp} B[\theta]$. If $y \neq x$, it is enough to show that $(\sigma\Sigma)(y) \Vdash_{\perp\!\!\!\perp} B[\theta]$ which is true since we have got $\sigma\Sigma \Vdash_{\perp\!\!\!\perp} \Gamma[\theta]$ by induction hypothesis. If $y = x$ we need to show that $(\sigma\Sigma + \{x \mapsto c\Sigma\})(x) = c\Sigma \Vdash_{\perp\!\!\!\perp} A[\theta]$, which is true by induction hypotesis.
- $<>_i$: we have a derivation of $\vdash \sigma : \Gamma$ and a derivation of $\Gamma \vdash t : A$, and we must show that $\langle t\,,\, \sigma\rangle\Sigma \Vdash_{\perp\!\!\!\perp} A[\theta]$. We know that Σ is a channel assignment for the term t, and by induction hypothesis we know that $\sigma\Sigma \Vdash_{\perp\!\!\!\perp} \Gamma[\theta]$, hence we can apply theorem 1 and get $\langle t\Sigma\,,\, \sigma\Sigma\rangle \Vdash_{\perp\!\!\!\perp} A[\theta]$, which is what we wanted to show.
- k_π: we have a derivation of $\vdash \pi : A^\perp$, and we must show that $k_{\pi\Sigma} \Vdash_{\perp\!\!\!\perp} (A \to B)[\theta]$. This is equivalent to showing that $k_{\pi\Sigma} \star \rho \in \perp\!\!\!\perp$ for every stack $\rho \in \|(A \to B)[\theta]\|_{\perp\!\!\!\perp}$. By

definition such stack ρ should have the form $d.\pi'$ with $d \in |A[\rho]|_{⫫}$ and $\pi' \in ||B[\theta]||_{⫫}$. Since $d \Vdash_{⫫} A[\theta]$ we know that for every stack $\rho' \in ||A[\theta]||_{\perp}$, $d \star \rho' \in ⫫$. By induction hypothesis we know that $\pi\Sigma \in ||A[\theta]||_{⫫}$, and hence $d \star \pi\Sigma \in ⫫$. Since $k_{\pi\Sigma} \star d.\pi' \succ d \star \pi\Sigma$, and since $⫫$ is closed under anti-evaluation, we get that $k_{\pi\Sigma} \star \rho \in ⫫$ for every stack $\rho = d.\pi' \in ||(A \to B)[\theta]||_{⫫}$.

- ε: this case is trivial since for every $N \in \mathscr{B}$, $\varepsilon\Sigma = \varepsilon \in ||N[\theta]|| = I_N$ by definition.
- π: we have a derivation of $\vdash c : A$ and a derivation of $\vdash \pi : B^{\perp}$, and we must show that $(c.\pi)\Sigma \in ||(A \to B)[\theta]||_{⫫}^{\perp}$. By induction hypothesis we know that $\pi\Sigma \in ||B[\theta]||_{⫫}$, and that $c\Sigma \Vdash_{⫫} A[\theta]$, which is equivalent to $c \in |A[\theta]|_{⫫}$ by definition. This gives us $c.\pi \in ||(A \to B)[\theta]||_{⫫}$. □

Corollary 1. Let $⫫$ be a fixed pole and Σ be a channel assignment for a process p. If $\vdash p : \perp$ then $p\Sigma \in ⫫$.

Proof. Like every process, p has the form $c \star \pi$. Since $\vdash c \star \pi : \perp$, we can apply the $\star$ typing rule to obtain $\vdash c : A$ and $\vdash \pi : A^{\perp}$ for some type A. Since $\vdash c : A$, we can apply theorem 2 and obtain $c \Vdash_{dbotA} [\theta]$ for any valuation θ such that $A[\theta]$ is a closed parametric formula. By definition, this means that $c \star \rho \in ⫫$ for every stack $\rho \in ||A[\theta]||$. Now by applying theorem 2 again on $\vdash \pi : A^{\perp}$ we obtain that $\pi \in ||A[\theta]||$ which precisely means that $p \in ⫫$. □

Normalization of Typed Processes

We would now like to reason about processes that contain channels, and interpret them in terms of realizability. Until now, we always applied a channel substitution to terms, closures and processes in general. However, it is possible to enforce that a channel realizes its type by constraining the pole, and thus get rid of the channel substitution.

Definition 4. We say that a pole $⫫$ is channel-preserving if for every channel $[\alpha : \Delta \Rightarrow A]$, every valuation θ such that $\Delta[\theta]$ is a closed parametric context and $A[\theta]$ is a closed parametric formula, and every environment σ such that $\sigma \Vdash_{⫫} \Delta[\theta]$, we have $\langle [\alpha : \Delta \Rightarrow A], \sigma \rangle \Vdash_{⫫} A[\theta]$.

Definition 5. The identity channel substitution is defined to be a channel substitution Σ_{id} such that for every term, environment, closure, stack or process Ψ, $\Psi\Sigma_{id} = \Psi$.

Theorem 3. Let $⫫$ be a channel-preserving pole, σ be an environment, and θ be a valuation such that $\Gamma[\theta]$ is a closed parametric context and $A[\theta]$ is a closed parametric formula. If the judgement $\Gamma \vdash t : A$ is provable and if $\sigma \Vdash_{⫫} \Gamma[\theta]$, then $\langle t, \sigma \rangle \Vdash_{⫫} A[\theta]$.

Proof. Since $\perp\!\!\!\perp$ is channel-preserving, Σ_{id} is a channel substitution for t. We can then apply theorem 1. □

Theorem 4. Let $\perp\!\!\!\perp$ be a channel-preserving pole, and θ be a valuation such that $A[\theta]$ is a closed parametric formula and $\Gamma[\theta]$ is a closed parametric context.

1. If $\vdash c : A$ is provable, then $c \Vdash_{\perp\!\!\!\perp} A[\theta]$.
2. If $\vdash \sigma : \Gamma$ is provable, then $\sigma \Vdash_{\perp\!\!\!\perp} \Gamma[\theta]$.
3. If $\vdash \pi : A^{\perp}$ is provable, then $\pi \in \|A[\theta]\|_{\perp\!\!\!\perp}$.

Proof. Since $\perp\!\!\!\perp$ is channel-preserving, Σ_{id} is a channel substitution for c, σ and π. We can then apply theorem 2. □

Corollary 2. Let $\perp\!\!\!\perp$ be a channel-preserving pole. If $\vdash p : \perp$ then $p \in \perp\!\!\!\perp$.

Proof. Since $\perp\!\!\!\perp$ is channel-preserving, Σ_{id} is a channel substitution for p. We can then apply corollary 1. □

Definition 6. A final state is a process p such that there exists no $q \in \Lambda\star\Pi$ such that $p \succ q$. We denote $\mathscr{F} \subset \Lambda\star\Pi$ the set of all final states.

Definition 7. The set of final states $\mathscr{F}$ is partitioned into three sets:

- the set of channel states $\mathscr{C}$ which contains all the processes of the form $\langle[\alpha : \Delta \Rightarrow A], \sigma\rangle\star\pi$,
- the set of bad final states $\mathscr{B}$ which contains all the processes of the form $\langle\lambda x . t, \sigma\rangle\star\varepsilon$ and all the processes of the form $k_{\pi}\star\varepsilon$,
- and the set of good final states $\mathscr{G}$ which contains the remaining final states.

Let us now consider the pole:

$$\perp\!\!\!\perp_{\mathscr{N}} = \{p \mid \exists q \in \mathscr{G} \cup \mathscr{C}\ \ p \succ q\}$$

It is clearly channel-preserving since for every channel $[\alpha]$, substitution σ, and stack π, we have $\langle[\alpha], \sigma\rangle\star\pi \in \mathscr{F} \subset \perp\!\!\!\perp_{\mathscr{F}}$. The pole $\perp\!\!\!\perp_{\mathscr{N}}$ can be used to show that the $\succ$ relation is normalizing for typed processes.

Theorem 5. If p is a process such that $\vdash p : \perp$, then there must exist $q \in \mathscr{G} \cup \mathscr{C}$ such that $p \succ^{*} q$.

Proof. Since $\vdash p : \perp$ and $\perp\!\!\!\perp_{\mathscr{N}}$ is channel-preserving, we can apply corollary 2 and obtain that $p \in \mathscr{N}$. This precisely means that $p \succ^{*} q \in \mathscr{G} \cup \mathscr{C}$. □

Atomic Normal Forms and Reduction

Definition 8. A channel $[\alpha : \Delta \Rightarrow A]$ is associated to a set of so-called atomic normal forms (ANF), denoted $\mathrm{ANF}([\alpha : \Delta \Rightarrow A])$, and defined as follow, where $\{\beta_1 \ldots \beta_n, \beta, \gamma\} \subset \Lambda_\alpha$ are fresh channel names.

$$\mathrm{ANF}([\alpha : \Delta \Rightarrow A \to B]) = \{\lambda x.[\beta : \Delta, x : A \Rightarrow B]\} \\ \cup \{\mathbf{cc}\,[\gamma : \Delta \Rightarrow ((A \to B) \to C) \to (A \to B)] \mid C \text{ type}\}$$

$$\mathrm{ANF}([\alpha : \Delta \Rightarrow X]) = \left\{(x)\,[\beta_1 : \Delta \Rightarrow B_1] \ldots [\beta_n : \Delta \Rightarrow B_n] \mid x : \vec{B} \to X \in \Delta\right\} \\ \cup \{\mathbf{cc}\,[\gamma : \Delta \Rightarrow (X \to B) \to X] \mid B \text{ type}\}$$

$$\mathrm{ANF}([\alpha : \Delta \Rightarrow N]) = \left\{(x)\,[\beta_1 : \Delta \Rightarrow B_1] \ldots [\beta_n : \Delta \Rightarrow B_n] \mid x : \vec{B} \to N \in \Delta\right\} \\ \cup \{\mathbf{cc}\,[\gamma : \Delta \Rightarrow (N \to B) \to N] \mid B \text{ type}\}$$

We would now like to allow the channels to be reduced into their atomic normal forms. To do so, we define a new reduction relation.

Definition 9. The reduction relation $\twoheadrightarrow$ is defined to be the smallest relation such that $\succ \subseteq \twoheadrightarrow$ and that:

$$\langle [\alpha], \sigma \rangle \star \pi \twoheadrightarrow \langle p, \sigma \rangle \star \pi \qquad\qquad p \in \mathrm{ANF}([\alpha])$$

A remark that one can make about the ANFs is that they all respect, in some sense, the typing of the channel they are associated to. This is formalized in the following lemma.

Lemma 6. Let $[\Delta \vdash \alpha : A]$ be a channel. For every $p \in \mathrm{ANF}([\alpha])$ there exists a proof Q of the judgement $\Delta \vdash p : A$.

Proof. Let us pick $p \in \mathrm{ANF}([\Delta \vdash \alpha : A])$, and reason by case on the structure of the type A:

- If $A = B \to C$, then p can be of two forms:
  - $p = \mathbf{cc}\,[\Delta \vdash \gamma : ((A \to B) \to C) \to (A \to B)]$ for some type C. The following proof can be used as Q:

$$\dfrac{\dfrac{}{\Delta \vdash \mathbf{cc} : \mathscr{P}_{A \to B, C}}\,\mathbf{cc} \qquad \dfrac{\Delta \subseteq \Delta}{\Delta \vdash [\Delta \vdash \beta] : ((A \to B) \to C) \to (A \to B)}\,\mathrm{Ch}}{\Delta \vdash \mathbf{cc}\,[\Delta \vdash \beta : ((A \to B) \to C) \to (A \to B)] : A \to B}\,{\to_e}$$

- $p = \lambda x.[\Delta, x : B \vdash \beta : C]$. We can take the following proof as Q:

$$\dfrac{\dfrac{\Delta, x : B \subseteq \Delta, x : B}{\Delta, x : B \vdash [\Delta, x : B \vdash \beta : C] : C}\,\text{Ch}}{\Delta \vdash \lambda x.[\Delta, x : B \vdash \beta : C] : B \to C}\,\to_i$$

- If $A = X \in \mathscr{V}$, then p can be of two forms:
  - $p = \mathbf{cc}[\Delta \vdash \beta : (X \to B) \to X]$ for some type B. The following proof does the trick:

$$\dfrac{\dfrac{}{\Delta \vdash \mathbf{cc} : \mathscr{P}_{X,B}}\,\text{cc} \qquad \dfrac{\Delta \subseteq \Delta}{\Delta \vdash [\Delta \vdash \beta] : (X \to B) \to X}\,\text{Ch}}{\Delta \vdash \mathbf{cc}[\Delta \vdash \beta : (X \to B) \to X] : X}\,\to_e$$

  - $p = (x)[\Delta \vdash \beta_1 : B_1]\ldots[\Delta \vdash \beta_n : B_n]$ with $x : B_1 \ldots B_n \to X$ in Δ. In this case, the following proof does the trick:

$$\dfrac{\dfrac{}{\Delta \vdash x : B_1\ldots B_n \to X}\,\text{Ax} \qquad \dfrac{\Delta \subseteq \Delta}{\Delta \vdash [\beta_1] : B_1}\,\text{Ch} \qquad \cdots \qquad \dfrac{\Delta \subseteq \Delta}{\Delta \vdash [\beta_n] : B_n}\,\text{Ch}}{\Delta \vdash (x)[\beta_1]\ldots[\beta_{n-1}] : B_n \to X}\,(\to_e)^n$$

- If $A = N \in \mathscr{B}$, the proof is similar as for the case for $A = X \in \mathscr{V}$. □

Subject Reduction We can now state a subject reduction theorem for the relation $\twoheadrightarrow$. This show that the full reduction relation is compatible with the typing of processes, in the sense that it preserves it.

Theorem 7. If p is a processus such that $p \twoheadrightarrow q$ and $p : \bot$ is provable in the above type-system, then $q : \bot$ is also provable.

Proof. We show that the application of any of the six reduction rules of the machine preserves the typing property.

- We consider the processus $p = \langle x, \sigma + \{x \mapsto c\}\rangle \star \pi$, and we suppose that $\vdash p : \bot$. There must exist a proof P_1 of $\vdash \sigma : \Gamma$, a proof P_2 of $\vdash c : A$ and a proof P_3 of $\pi : A^\bot$ since a proof of $p = \langle x, \sigma + \{x \mapsto c\}\rangle \star \pi$ has the form:

$$\dfrac{\dfrac{\dfrac{\overset{P_1}{\vdots}}{\vdash \sigma : \Gamma} \quad \dfrac{\overset{P_2}{\vdots}}{\vdash c : A}}{\vdash \sigma + \{x \mapsto c\} : \Gamma, x : A}\,\sigma_+ \qquad \dfrac{}{\Gamma, x : A \vdash x : A}\,Ax}{\vdash \langle x, \sigma + \{x \mapsto c\}\rangle : A}\,<>_i \qquad \dfrac{\overset{P_3}{\vdots}}{\vdash \pi : A^\bot}}{\vdash \langle x, \sigma + \{x \mapsto c\}\rangle \star \pi : \bot}\,\star$$

Using P_2 and P_3, the following is a proof of $\vdash c \star \pi : \bot$:

$$\dfrac{\dfrac{\overset{P_2}{\vdots}}{\vdash c : A} \qquad \dfrac{\overset{P_3}{\vdots}}{\vdash \pi : A^\bot}}{\vdash c \star \pi : \bot}\,\star$$

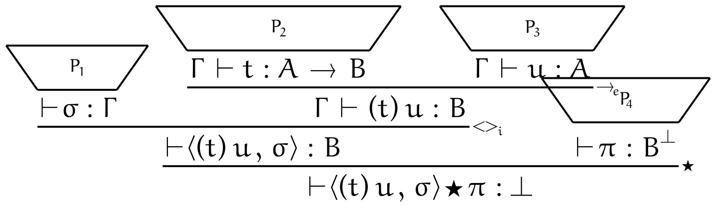
- We consider the processus $p = \langle \lambda x.t, \sigma\rangle \star c.\pi$, and we suppose that $\vdash p : \bot$. There must exist a proof P_1 of $\vdash \sigma : \Gamma$, a proof P_2 of $\Gamma, x : A \vdash t : B$, a proof P_3 of $\vdash c : A$ and a proof P_4 of $\vdash \pi : B^\bot$ since a proof of $\vdash \langle \lambda x.t, \sigma\rangle \star c.\pi : \bot$ has the form:

$$\dfrac{\dfrac{\dfrac{\overset{P_1}{\vdots}}{\vdash \sigma : \Gamma} \quad \dfrac{\dfrac{\overset{P_2}{\vdots}}{\Gamma, x : A \vdash t : B}}{\Gamma \vdash \lambda x.t : A \to B}\,\to_i}{\vdash \langle \lambda x.t, \sigma\rangle : A \to B}\,<>_i \qquad \dfrac{\dfrac{\overset{P_3}{\vdots}}{\vdash c : A} \quad \dfrac{\overset{P_4}{\vdots}}{\vdash \pi : B^\bot}}{\vdash c.\pi : (A \to B)^\bot}\,\pi}{\vdash \langle \lambda x.t, \sigma\rangle \star c.\pi : \bot}\,\star$$

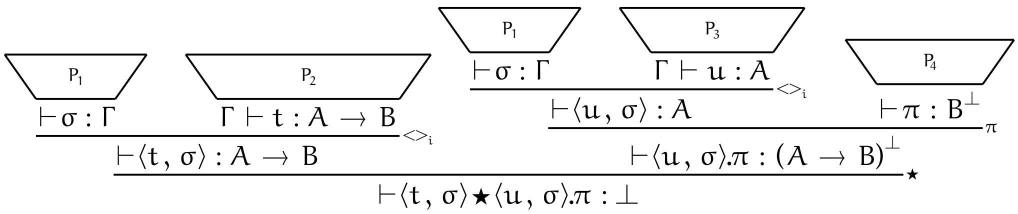
Using P_1, P_2, P_3 and P_4, the following is a proof of $\vdash \langle t, \sigma + x \mapsto c\rangle \star \pi : \bot$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\overset{P_1}{\vdots}}{\vdash \sigma : \Gamma} \quad \dfrac{\overset{P_3}{\vdots}}{\vdash c : A}}{\vdash \sigma + x \mapsto c : \Gamma, x : A}\,\sigma \qquad \dfrac{\overset{P_2}{\vdots}}{\Gamma, x : A \vdash t : B}}{\vdash \langle t, \sigma + x \mapsto c\rangle : B}\,<>_i \qquad \dfrac{\overset{P_4}{\vdots}}{\vdash \pi : B^\bot}}{\vdash \langle t, \sigma + x \mapsto c\rangle \star \pi : \bot}\,\star$$

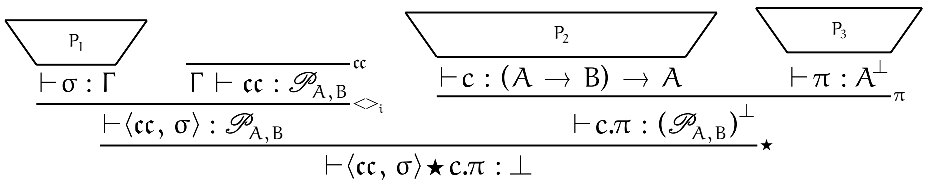
– We consider the processus $p = \langle (t)\,u\,,\,\sigma\rangle \star \pi$, and we suppose that $\vdash p : \bot$. There must exist a proof P_1 of $\vdash \sigma : \Gamma$, a proof P_2 of $\Gamma \vdash t : A \to B$, a proof P_3 of $\Gamma \vdash u : A$ and a proof P_4 of $\vdash \pi : B^\bot$ since a proof of $\vdash \langle (t)\,u\,,\,\sigma\rangle \star \pi : \bot$ has the form:



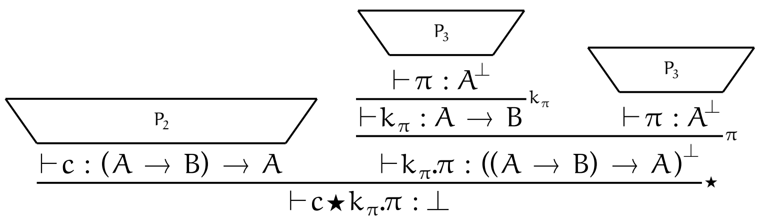
Using P_1, P_2, P_3 and P_4, the following is a proof of $\vdash \langle t\,,\,\sigma\rangle \star \langle u\,,\,\sigma\rangle.\pi : \bot$:



– We consider the processus $p = \langle \mathfrak{cc}\,,\,\sigma\rangle \star c.\pi$, and we suppose that $\vdash p : \bot$. There must exist a proof P_1 of $\vdash \sigma : \Gamma$, a proof P_2 of $\vdash c : (A \to B) \to A$ and a proof P_3 of $\vdash \pi : A^\bot$ since a proof of $\vdash \langle \mathfrak{cc}\,,\,\sigma\rangle \star c.\pi : \bot$ has the form:



Using P_2 and P_3, the following is a proof of $\vdash c \star k_\pi.\pi : \bot$:



- We consider the processus $p = k_\pi \star c.\pi'$, and we suppose that $\vdash p : \perp$. There must exist a proof P_1 of $\vdash \pi : A^\perp$, a proof P_2 of $\vdash c : A$ and a proof P_3 of $\vdash \pi' : B^\perp$ since a proof of $\vdash k_\pi \star c.\pi' : \perp$ has the form:

$$\dfrac{\dfrac{\dfrac{P_1}{\vdash \pi : A^\perp}}{\vdash k_\pi : A \to B}\,k_\pi \qquad \dfrac{\dfrac{P_2}{\vdash c : A} \qquad \dfrac{P_3}{\vdash \pi' : B^\perp}}{\Gamma \vdash c.\pi' : (A \to B)^\perp}\,\pi}{\vdash k_\pi \star c.\pi' : \perp}\,\star$$

Using P_1 and P_2, the following is a proof of $\vdash c \star \pi : \perp$:

$$\dfrac{\dfrac{P_2}{\vdash c : A} \qquad \dfrac{P_1}{\vdash \pi : A^\perp}}{\vdash c \star \pi : \perp}\,\star$$

- We consider the processus $p = \langle [\Delta \vdash \alpha : A], \sigma \rangle \star \pi$, and we suppose that $\vdash p : \perp$. There must exist a proof P_1 of $\vdash \sigma : \Gamma$ and a proof P_2 of $\vdash \pi : A^\perp$ since a proof of $\vdash \langle [\Delta \vdash \alpha : A], \sigma \rangle \star \pi : \perp$ has the form:

$$\dfrac{\dfrac{\dfrac{P_1}{\vdash \sigma : \Gamma} \qquad \dfrac{\Delta \subseteq \Gamma}{\Gamma \vdash [\Delta \vdash \alpha : A] : A}\,\mathrm{Ch}}{\vdash \langle [\Delta \vdash \alpha : A], \sigma \rangle : A}\,<>_i \qquad \dfrac{P_2}{\vdash \pi : A^\perp}}{\vdash \langle [\Delta \vdash \alpha : A], \sigma \rangle \star \pi : \perp}\,\star$$

Let us take $p \in \mathrm{ANF}([\alpha])$ and Q a proof of $\Delta \vdash p : A$ given by lemma 1. Using P_1 and P_2 the following is a proof of $\vdash \langle p, \sigma \rangle \star \pi : \perp$:

$$\dfrac{\dfrac{\dfrac{P_1}{\vdash \sigma : \Gamma} \qquad \dfrac{\dfrac{Q}{\Delta \vdash p : A}}{\Gamma \vdash p : A}\,\mathrm{Wk}}{\vdash \langle p, \sigma \rangle : A}\,<>_i \qquad \dfrac{P_2}{\vdash \pi : A^\perp}}{\vdash \langle p, \sigma \rangle \star \pi : \perp}\,\star$$

□

The Reduction of Channels is Well-Behaved

We wish to show that when the machine is reducing a term containing channels, it will satisfy the two following criterion:

- it will never stop on a bad final state (i.e an element of $\mathscr{B}$)
- and if it never stops, it will go through infinitely many channel states (i.e elements of $\mathscr{C}$).

Theorem 8. Let p be a process such that $\vdash p : \perp$. There is no process $q \in \mathscr{B}$ such that $p \twoheadrightarrow^* q$.

Proof. Let us suppose that $p \twoheadrightarrow^* q \in \mathscr{B}$. The subject reduction theorem tells us that $\vdash q : \perp$. By applying theorem 5 we know that there is a process $q' \in \mathscr{G} \cup \mathscr{C}$ such that $q \succ^* q'$. However, the only process q' such that $q \succ^* q'$ is q itself. We thus obtain a contradiction since $\mathscr{B}$ and $\mathscr{G} \cup \mathscr{C}$ are disjoint. □

Theorem 9. Let p be a process such that $\vdash p : \perp\!\!\!\perp$, and $P : (p_i)_{i \in \mathbb{N}}$ be a sequence of processes such that $p_0 = p$ and $\forall i \in \mathbb{N}\ p_i \twoheadrightarrow p_{i+1}$. There exists a subsequence $Q : (q_i)_{i \in \mathbb{N}}$ of P such that $\forall i \in \mathbb{N}\ q_i \in \mathscr{C}$.

Proof. Let us suppose that we have built the n first elements of Q. This means that $q_0 = p_{k_0} \dots q_n = p_{k_n}$ with $k_0 < \dots < k_n$ and $q_0 \dots q_n \in \mathscr{C}$. We consider the process $q_n = p_{k_n}$, which has the form $\langle [\alpha], \sigma \rangle \star \pi$ since $q_n \in \mathscr{C}$. We now consider the process p_{k_n+1}, which has the form $\langle a, \sigma \rangle \star \pi$ with $a \in \mathrm{ANF}([\alpha])$ (by definition $p_{k_n} \twoheadrightarrow p_{k_n+1}$). We now need to find $k > k_n$ such that $p_k \in \mathscr{C}$, if we succeed we will be able to conclude by taking $q_{n+1} = p_k$. Since $p \vdash \perp$ and $p \twoheadrightarrow^* \langle a, \sigma \rangle \star \pi$, we can use the subject reduction theorem to show that $\langle a, \sigma \rangle \star \pi \vdash \perp$. Now, by theorem 5, there must exist $q \in \mathscr{G} \cup \mathscr{C}$ such that $\langle a, \sigma \rangle \star \pi \succ^* q$. This means that we have a unique q such that $\langle a, \sigma \rangle \star \pi \twoheadrightarrow^* q$, hence the sequence P has to go through q. It remains to show that $q \notin \mathscr{G}$. Let us suppose that $q \in \mathscr{G}$, which means that there is no process q' such that $q \succ q'$. This cannot be the case since it contradicts the definition of the sequence P. □