Rule Formats for Nominal Transition Systems

Luca Aceto, Ignacio Fábregas, **Álvaro García-Pérez**,
Anna Ingólfsdóttir and Yolanda Ortega-Mallén

September 8th, 2017

Rule Formats for Nominal Transition Systems

Rule Formats for Nominal Transition Systems

A rose by any other name would smell as sweet.

Romeo Montague

Countably many atoms $a, b, \ldots \in \mathbb{A}$.

Countably many atoms $a, b, \ldots \in \mathbb{A}$.

Finite permutations of atoms $\pi = (a_1\ b_1) \circ \ldots \circ (a_k\ b_k) \in \mathrm{Perm}\ \mathbb{A}$.

Countably many atoms $a, b, \ldots \in \mathbb{A}$.

Finite permutations of atoms $\pi = (a_1\ b_1) \circ \ldots \circ (a_k\ b_k) \in \mathrm{Perm}\ \mathbb{A}$.

$$(\nu b)(\overline{a}b.0)$$

Countably many atoms $a, b, \ldots \in \mathbb{A}$.

Finite permutations of atoms $\pi = (a_1\ b_1) \circ \ldots \circ (a_k\ b_k) \in \mathrm{Perm}\ \mathbb{A}$.

$(\nu b)(\overline{a}b.0)$

Countably many atoms $a, b, \ldots \in \mathbb{A}$.

Finite permutations of atoms $\pi = (a_1\ b_1) \circ \ldots \circ (a_k\ b_k) \in \mathrm{Perm}\ \mathbb{A}$.

$$(b\,c) \cdot (\nu b)(\overline{a}b.0)$$

Countably many atoms $a, b, \ldots \in \mathbb{A}$.

Finite permutations of atoms $\pi = (a_1\ b_1) \circ \ldots \circ (a_k\ b_k) \in \mathrm{Perm}\ \mathbb{A}$.

$$(\nu c)(\overline{a}c.0)$$

Countably many atoms $a, b, \ldots \in \mathbb{A}$.

Finite permutations of atoms $\pi = (a_1\ b_1) \circ \ldots \circ (a_k\ b_k) \in \mathrm{Perm}\ \mathbb{A}$.

$$(\nu c)(\overline{a}c.0) =_\alpha (\nu b)(\overline{a}b.0)$$

Countably many atoms $a, b, \ldots \in \mathbb{A}$.

Finite permutations of atoms $\pi = (a_1\ b_1) \circ \ldots \circ (a_k\ b_k) \in \mathrm{Perm}\ \mathbb{A}$.

$$(\nu b)(\overline{a}b.0)$$

Countably many atoms $a, b, \ldots \in \mathbb{A}$.

Finite permutations of atoms $\pi = (a_1\ b_1) \circ \ldots \circ (a_k\ b_k) \in \mathrm{Perm}\ \mathbb{A}$.

$(\nu b)(\bar{a}b.0)$

Countably many atoms $a, b, \ldots \in \mathbb{A}$.

Finite permutations of atoms $\pi = (a_1\ b_1) \circ \ldots \circ (a_k\ b_k) \in \mathrm{Perm}\ \mathbb{A}$.

$$(a\,c) \cdot (\nu b)(\overline{a} b.0)$$

Countably many atoms $a, b, \ldots \in \mathbb{A}$.

Finite permutations of atoms $\pi = (a_1\ b_1) \circ \ldots \circ (a_k\ b_k) \in \mathrm{Perm}\ \mathbb{A}$.

$$(\nu b)(\overline{c} b.0)$$

Countably many atoms $a, b, \ldots \in \mathbb{A}$.

Finite permutations of atoms $\pi = (a_1\ b_1) \circ \ldots \circ (a_k\ b_k) \in \mathrm{Perm}\ \mathbb{A}$.

$$(\nu b)(\overline{c}b.0) \neq_\alpha (\nu b)(\overline{a}b.0)$$

Countably many atoms $a, b, \ldots \in \mathbb{A}$.

Finite permutations of atoms $\pi = (a_1\ b_1) \circ \ldots \circ (a_k\ b_k) \in \mathrm{Perm}\ \mathbb{A}$.

$$(\nu b)(\overline{c}b.0) \neq_\alpha (\nu b)(\overline{a}b.0)$$

$$a \in \mathrm{supp}((\nu b)(\overline{a}b.0))$$

Countably many atoms $a, b, \ldots \in \mathbb{A}$.

Finite permutations of atoms $\pi = (a_1\ b_1) \circ \ldots \circ (a_k\ b_k) \in \mathrm{Perm}\ \mathbb{A}$.

$$(\nu b)(\overline{c}b.0) \neq_\alpha (\nu b)(\overline{a}b.0)$$

$$a \in \mathrm{supp}((\nu b)(\overline{a}b.0))$$

$$b\#(\nu b)(\overline{a}b.0)$$

Countably many atoms $a, b, \ldots \in \mathbb{A}$.

Finite permutations of atoms $\pi = (a_1\ b_1) \circ \ldots \circ (a_k\ b_k) \in \mathrm{Perm}\ \mathbb{A}$.

$$(\nu b)(\overline{c}b.0) \neq_\alpha (\nu b)(\overline{a}b.0)$$

$$a \in \mathrm{supp}((\nu b)(\overline{a}b.0))$$

$$b\#(\nu b)(\overline{a}b.0) \quad \text{iff} \quad b \notin \mathrm{supp}((\nu b)(\overline{a}b.0))$$

Nominal set

A *nominal set* S is a $\mathrm{Perm}\ \mathbb{A}$-set whose elements have finite support.

Nominal set

A *nominal set* S is a $\mathrm{Perm}\ \mathbb{A}$-set whose elements have finite support.

Finitely supported functions are elements of nominal sets.

$$(\pi \cdot f)(s) = \pi \cdot (f(\pi^{-1} \cdot s)).$$

Nominal set

A *nominal set* S is a $\mathrm{Perm}\ \mathbb{A}$-set whose elements have finite support.

Finitely supported functions are elements of nominal sets.

$$(\pi \cdot f)(s) = \pi \cdot (f(\pi^{-1} \cdot s)).$$

Equivariant function

A function f is *equivariant* if $\pi \cdot (f(s)) = f(\pi \cdot s)$ for every $\pi \in \mathrm{Perm}\ \mathbb{A}$.

Nominal set

A *nominal set* S is a $\mathrm{Perm}\ \mathbb{A}$-set whose elements have finite support.

Finitely supported functions are elements of nominal sets.

$$(\pi \cdot f)(s) = \pi \cdot (f(\pi^{-1} \cdot s)).$$

Equivariant function

A function f is *equivariant* if $\pi \cdot (f(s)) = f(\pi \cdot s)$ for every $\pi \in \mathrm{Perm}\ \mathbb{A}$.

Atom abstraction

$\langle a \rangle s = \{(b, (b\,a) \cdot s) \mid b = a \vee b \# s\}$ where $a \in \mathbb{A}$ and $s \in S$.

Nominal set

A *nominal set* S is a $\mathrm{Perm}\ \mathbb{A}$-set whose elements have finite support.

Finitely supported functions are elements of nominal sets.

$$(\pi \cdot f)(s) = \pi \cdot (f(\pi^{-1} \cdot s)).$$

Equivariant function

A function f is *equivariant* if $\pi \cdot (f(s)) = f(\pi \cdot s)$ for every $\pi \in \mathrm{Perm}\ \mathbb{A}$.

Atom abstraction

$\langle a \rangle s = \{(b, (b\,a) \cdot s) \mid b = a \vee b \# s\}$ where $a \in \mathbb{A}$ and $s \in S$.

$$\begin{aligned} \pi \cdot \langle a \rangle s &= \langle \pi \cdot a \rangle (\pi \cdot s) \\ \mathrm{supp}(\langle a \rangle s) &= \mathrm{supp}(s) \setminus \{a\}. \end{aligned}$$

Rule Formats for Nominal Transition Systems

Nominal transition system [Parrow et al., 2015]

Quadruple $(S, Act, \mathrm{bn}, \longrightarrow)$ where

(i) S and Act are nominal sets of *states* and *actions* respectively,

(ii) $\longrightarrow \subseteq S \times (Act \times S)$ is an equivariant binary *transition relation* from states to *residuals*,

Nominal transition system [Parrow et al., 2015]

Quadruple $(S, Act, \mathrm{bn}, \longrightarrow)$ where

(i) S and Act are nominal sets of *states* and *actions* respectively,

(ii) $\longrightarrow \subseteq S \times (Act \times S)$ is an equivariant binary *transition relation* from states to *residuals*,

(iii) $\mathrm{bn} : Act \to \mathcal{P}_\omega(\mathbb{A})$ is an equivariant function from actions to finite sets of *binding names*, and

(iv) $\longrightarrow$ satisfies *alpha-conversion of residuals*:
If $p \xrightarrow{\ell} p'$, $b \in \mathrm{bn}(\ell)$ and c fresh in (ℓ, p') then $p \xrightarrow{(b\,c)\cdot\ell} (b\,c) \cdot p'$.

Nominal transition system [Parrow et al., 2015]

Quadruple $(S, Act, \mathrm{bn}, \longrightarrow)$ where

(i) S and Act are nominal sets of *states* and *actions* respectively,

(ii) $\longrightarrow \subseteq S \times (Act \times S)$ is an equivariant binary *transition relation* from states to *residuals*,

(iii) $\mathrm{bn} : Act \to \mathcal{P}_\omega(\mathbb{A})$ is an equivariant function from actions to finite sets of *binding names*, and

(iv) $\longrightarrow$ satisfies *alpha-conversion of residuals*:
If $p \xrightarrow{\ell} p'$, $b \in \mathrm{bn}(\ell)$ and c fresh in (ℓ, p') then $p \xrightarrow{(b\,c)\cdot\ell} (b\,c) \cdot p'$.

$$(\nu b)(\overline{a}b.p) \xrightarrow{\overline{a}(\nu b)} p'$$

Nominal transition system [Parrow et al., 2015]

Quadruple $(S, Act, \mathrm{bn}, \longrightarrow)$ where

(i) S and Act are nominal sets of *states* and *actions* respectively,

(ii) $\longrightarrow \subseteq S \times (Act \times S)$ is an equivariant binary *transition relation* from states to *residuals*,

(iii) $\mathrm{bn} : Act \to \mathcal{P}_\omega(\mathbb{A})$ is an equivariant function from actions to finite sets of *binding names*, and

(iv) $\longrightarrow$ satisfies *alpha-conversion of residuals*:
If $p \xrightarrow{\ell} p'$, $b \in \mathrm{bn}(\ell)$ and c fresh in (ℓ, p') then $p \xrightarrow{(b\,c)\cdot\ell} (b\,c) \cdot p'$.

$$(\nu b)(\overline{a}b.p) \xrightarrow{\overline{a}(\nu b)} p'$$

Nominal transition system [Parrow et al., 2015]

Quadruple $(S, Act, \mathrm{bn}, \longrightarrow)$ where

(i) S and Act are nominal sets of *states* and *actions* respectively,

(ii) $\longrightarrow \subseteq S \times (Act \times S)$ is an equivariant binary *transition relation* from states to *residuals*,

(iii) $\mathrm{bn} : Act \to \mathcal{P}_\omega(\mathbb{A})$ is an equivariant function from actions to finite sets of *binding names*, and

(iv) $\longrightarrow$ satisfies *alpha-conversion of residuals*:
If $p \xrightarrow{\ell} p'$, $b \in \mathrm{bn}(\ell)$ and c fresh in (ℓ, p') then $p \xrightarrow{(b\,c)\cdot\ell} (b\,c) \cdot p'$.

$$(\nu b)(\overline{a}b.p) \xrightarrow{\overline{a}(\nu c)} (b\,c) \cdot p'$$

Raw terms

$$t_\sigma ::= x_\sigma \mid a_\alpha \mid (\pi \bullet t_\sigma)_\sigma \mid ([a_\alpha]t_\sigma)_{[\alpha]\sigma} \mid (t_{\sigma_1}, \ldots, t_{\sigma_k})_{\sigma_1 \times \ldots \times \sigma_k} \mid (f(t_\sigma))_\delta$$

Raw terms

$t_\sigma ::= x_\sigma \mid a_\alpha \mid (\pi \bullet t_\sigma)_\sigma \mid ([a_\alpha]t_\sigma)_{[\alpha]\sigma} \mid (t_{\sigma_1}, \ldots, t_{\sigma_k})_{\sigma_1 \times \ldots \times \sigma_k} \mid (f(t_\sigma))_\delta$

$$\begin{aligned} \pi \cdot (\pi_1 \bullet t) &= (\pi \cdot \pi_1) \bullet (\pi \cdot t) \\ \mathrm{supp}(\pi_1 \bullet t) &= \mathrm{supp}(\pi_1) \cup \mathrm{supp}(t) \end{aligned}$$

$$\begin{aligned} \pi \cdot [a]t &= [\pi\, a](\pi \cdot t) \\ \mathrm{supp}([a]t) &= \{a\} \cup \mathrm{supp}(t) \end{aligned}$$

Substitution

$$
\begin{array}{rcl}
\varphi(x) & = & \varphi\, x \\
\varphi(a) & = & a \\
\varphi(\pi \bullet t) & = & \pi \bullet \varphi(t) \\
\varphi([a]t) & = & [a](\varphi(t)) \\
\varphi(t_1, \ldots, t_k) & = & (\varphi(t_1), \ldots, \varphi(t_k)) \\
\varphi(f(t)) & = & f(\varphi(t))
\end{array}
$$

The action of substitution is equivariant, i.e., $\pi \cdot \varphi(t) = \varphi^{\pi}(\pi \cdot t)$.

Σ-structure for nominal terms

Adapted from [Clouston and Pitts, 2007].

$$
\begin{aligned}
NT[\![a]\!] &= a \\
NT[\![\pi \bullet p]\!] &= \pi \cdot NT[\![p]\!] \\
NT[\![[a]p]\!] &= \langle a \rangle (NT[\![p]\!]) \\
NT[\![(p_1, \ldots, p_k)]\!] &= (NT[\![p_1]\!], \ldots, NT[\![p_k]\!]) \\
NT[\![f(p)]\!] &= NT[\![f]\!](NT[\![p]\!]).
\end{aligned}
$$

Nominal terms

Interpretations of ground terms in NT coincide with the nominal algebraic datatypes of [Pitts, 2013].

Base sorts $\Delta = \{\mathsf{pr}, \mathsf{ac}\}$, atom sorts $A = \{\mathsf{ch}\}$ and

$$
\begin{aligned}
F = \{\ & \mathit{null} : \mathbf{1} \to \mathsf{pr}, \\
& \mathit{tau} : \mathsf{pr} \to \mathsf{pr}, \\
& \mathit{in} : (\mathsf{ch} \times [\mathsf{ch}]\mathsf{pr}) \to \mathsf{pr}, \\
& \mathit{out} : (\mathsf{ch} \times \mathsf{ch} \times \mathsf{pr}) \to \mathsf{pr}, \\
& \mathit{par} : (\mathsf{pr} \times \mathsf{pr}) \to \mathsf{pr}, \\
& \mathit{sum} : (\mathsf{pr} \times \mathsf{pr}) \to \mathsf{pr}, \\
& \mathit{rep} : \mathsf{pr} \to \mathsf{pr}, \\
& \mathit{new} : [\mathsf{ch}]\mathsf{pr} \to \mathsf{pr}, \\
& \mathit{tauA} : \mathbf{1} \to \mathsf{ac}, \\
& \mathit{inA} : (\mathsf{ch} \times \mathsf{ch}) \to \mathsf{ac}, \\
& \mathit{outA} : (\mathsf{ch} \times \mathsf{ch}) \to \mathsf{ac}, \\
& \mathit{boutA} : (\mathsf{ch} \times \mathsf{ch}) \to \mathsf{ac} \quad \}.
\end{aligned}
$$

$$
NT[\![\mathit{new}([b](\mathit{out}(a, b, \mathit{null})))]\!] \longrightarrow NT[\![(\mathit{boutA}(a, b), \mathit{null})]\!]
$$

$$
\text{stands for} \qquad (\nu b)(\overline{a}b.\mathbf{0}) \xrightarrow{\overline{a}(\nu b)} \mathbf{0}
$$

Specification systems

$$\frac{\{u_i \longrightarrow u_i' \mid i \in I\} \quad \{a_j \not\approx v_j \mid j \in J\}}{t \longrightarrow t'}\ \mathsf{Ru}$$

Specification systems

$$\frac{\{u_i \longrightarrow u_i' \mid i \in I\} \quad \{a_j \not\approx v_j \mid j \in J\}}{t \longrightarrow t'}\ \mathsf{Ru}$$

$$\pi \cdot \mathsf{Ru}$$

$$NT[\![new([b](out(a, b, null)))]\!] \longrightarrow NT[\![(boutA(a, b), null)]\!]$$

$$NT[\![new([b](out(a,b,null)))]\!] \longrightarrow NT[\![(boutA(a,b),null)]\!]$$

$$\frac{x \longrightarrow (outA(a,b),y) \qquad b \not\approx a}{new([b]x) \longrightarrow (boutA(a,b),y)}\ (\mathsf{Open}) \qquad \begin{array}{lcl} \varphi_1(x) & = & out(a,b,null) \\ \varphi_1(y) & = & null \end{array}$$

$$\frac{}{NT[\![new([b](out(a,b,null)))]\!] \longrightarrow NT[\![(boutA(a,b),null)]\!]}\ (\text{Open})\ \text{and}\ b\#a$$

$$\frac{x \longrightarrow (outA(a,b),y) \qquad b \not\# a}{new([b]x) \longrightarrow (boutA(a,b),y)}\ (\text{Open}) \qquad \begin{array}{lcl} \varphi_1(x) & = & out(a,b,null) \\ \varphi_1(y) & = & null \end{array}$$

$$\frac{NT[\![out(a,b,null)]\!] \longrightarrow NT[\![(outA(a,b),null)]\!]}{NT[\![new([b](out(a,b,null)))]\!] \longrightarrow NT[\![(boutA(a,b),null)]\!]}\ \text{(Open) and } b\#a$$

$$\frac{x \longrightarrow (outA(a,b),y) \qquad b \not\approx a}{new([b]x) \longrightarrow (boutA(a,b),y)}\ \text{(Open)} \qquad \begin{array}{lcl} \varphi_1(x) & = & out(a,b,null) \\ \varphi_1(y) & = & null \end{array}$$

$$\frac{NT[\![out(a,b,null)]\!] \longrightarrow NT[\![(outA(a,b),null)]\!]}{NT[\![new([b](out(a,b,null)))]\!] \longrightarrow NT[\![(boutA(a,b),null)]\!]}\ \text{(Open) and } b\#a$$

$$\frac{}{out(a,b,x) \longrightarrow (outA(a,b),x)}\ \text{(Out)} \qquad \varphi_2(x) \quad = \quad null$$

$$\frac{\dfrac{}{NT[\![out(a,b,null)]\!] \longrightarrow NT[\![(outA(a,b),null)]\!]}\ (\text{Out})}{NT[\![new([b](out(a,b,null)))]\!] \longrightarrow NT[\![(boutA(a,b),null)]\!]}\ (\text{Open}) \text{ and } b\#a$$

$$\frac{}{out(a,b,x) \longrightarrow (outA(a,b),x)}\ (\text{Out}) \qquad \varphi_2(x) \quad = \quad null$$

$$\frac{\dfrac{}{NT[\![out(a,b,null)]\!] \longrightarrow NT[\![(outA(a,b),null)]\!]}\ (\text{Out})}{NT[\![new([b](out(a,b,null)))]\!] \longrightarrow NT[\![(boutA(a,b),null)]\!]}\ (\text{Open}) \text{ and } b\#a$$

$$\frac{}{out(a,b,x) \longrightarrow (outA(a,b),x)}\ (\text{Out}) \qquad \varphi_2(x) \quad = \quad null$$

$$\frac{\dfrac{}{NT[\![out(a,b,null)]\!] \longrightarrow NT[\![(outA(a,b),null)]\!]}\ (\text{Out})}{NT[\![new([c](out(a,c,null)))]\!] \longrightarrow NT[\![(boutA(a,b),null)]\!]}\ (\text{Open}) \text{ and } b\#a$$

$$\frac{}{out(a,b,x) \longrightarrow (outA(a,b),x)}\ (\text{Out}) \qquad \varphi_2(x) \quad = \quad null$$

$$\dfrac{\dfrac{}{NT[\![out(a,b,null)]\!] \longrightarrow NT[\![(outA(a,b),null)]\!]}\,(\text{Out})}{NT[\![new([c](out(a,c,null)))]\!] \longrightarrow NT[\![(boutA(a,b),null)]\!]}\,(\text{Open})\ \text{and}\ b\#a$$

$$\dfrac{}{out(a,b,x) \longrightarrow (outA(a,b),x)}\,(\text{Out}) \qquad \varphi_2(x) \;=\; null$$

Framework stems from [Urban et al., 2004, Clouston and Pitts, 2007, Fernández and Gabbay, 2007, Cimini et al., 2012, Pitts, 2013].

Rule Formats for Nominal Transition Systems

Easy-to-check, syntactic conditions over the rules of the inference system that ensure a property of interest in the induced transition relation.

Rule Formats for Nominal Transition Systems

Let $\mathcal{R}$ be a specification system which induces a transition system $\mathcal{T}$.
Is $\mathcal{T}$ equivariant?

Let $\mathcal{R}$ be a specification system which induces a transition system $\mathcal{T}$.
Is $\mathcal{T}$ equivariant?

Equivariant format

$\mathcal{R}$ is in *equivariant format* iff the rule $(a\,b) \cdot \mathrm{Ru}$ is in $\mathcal{R}$, for every rule Ru in $\mathcal{R}$ and for each $a, b \in \mathbb{A}$.

Let $\mathcal{R}$ be a specification system which induces a transition system $\mathcal{T}$.
Is $\mathcal{T}$ equivariant?

Equivariant format

$\mathcal{R}$ is in *equivariant format* iff the rule $(a\,b) \cdot \mathrm{Ru}$ is in $\mathcal{R}$, for every rule Ru in $\mathcal{R}$ and for each $a, b \in \mathbb{A}$.

Let bn be an equivariant binding-names function.
Does $\mathcal{T}$ satisfy alpha-conversion of residuals with respect to bn?

Simplification of frehsness environments

Adapted from [Fernández and Gabbay, 2007].

$$
\begin{array}{rcl}
\{a \not\approx b\} \cup \nabla & \Longrightarrow & \nabla \\
\{a \not\approx \pi \bullet t\} \cup \nabla & \Longrightarrow & \{\pi^{-1} \cdot a \not\approx t\} \cup \nabla \\
\{a \not\approx [b]p\} \cup \nabla & \Longrightarrow & \{a \not\approx p\} \cup \nabla \\
\{a \not\approx [a]p\} \cup \nabla & \Longrightarrow & \nabla \\
\{a \not\approx f(p)\} \cup \nabla & \Longrightarrow & \{a \not\approx p\} \cup \nabla \\
\{a \not\approx (p_1, \ldots, p_k)\} \cup \nabla & \Longrightarrow & \{a \not\approx p_i, \ldots, a \not\approx p_k\} \cup \nabla.
\end{array}
$$

Simplification of frehsness environments

Adapted from [Fernández and Gabbay, 2007].

$$
\begin{array}{rcl}
\{a \not\# b\} \cup \nabla & \Longrightarrow & \nabla \\
\{a \not\# \pi \bullet t\} \cup \nabla & \Longrightarrow & \{\pi^{-1} \cdot a \not\# t\} \cup \nabla \\
\{a \not\# [b]p\} \cup \nabla & \Longrightarrow & \{a \not\# p\} \cup \nabla \\
\{a \not\# [a]p\} \cup \nabla & \Longrightarrow & \nabla \\
\{a \not\# f(p)\} \cup \nabla & \Longrightarrow & \{a \not\# p\} \cup \nabla \\
\{a \not\# (p_1, \ldots, p_k)\} \cup \nabla & \Longrightarrow & \{a \not\# p_i, \ldots, a \not\# p_k\} \cup \nabla.
\end{array}
$$

Entailment

$\nabla \vdash \nabla'$ iff $\langle \nabla \rangle_{nf} \supseteq \langle \nabla' \rangle_{nf}$.

Simplification of frehsness environments

Adapted from [Fernández and Gabbay, 2007].

$$
\begin{array}{rcl}
\{a \not\# b\} \cup \nabla & \Longrightarrow & \nabla \\
\{a \not\# \pi \bullet t\} \cup \nabla & \Longrightarrow & \{\pi^{-1} \cdot a \not\# t\} \cup \nabla \\
\{a \not\# [b]p\} \cup \nabla & \Longrightarrow & \{a \not\# p\} \cup \nabla \\
\{a \not\# [a]p\} \cup \nabla & \Longrightarrow & \nabla \\
\{a \not\# f(p)\} \cup \nabla & \Longrightarrow & \{a \not\# p\} \cup \nabla \\
\{a \not\# (p_1, \ldots, p_k)\} \cup \nabla & \Longrightarrow & \{a \not\# p_i, \ldots, a \not\# p_k\} \cup \nabla.
\end{array}
$$

Entailment

$\nabla \vdash \nabla'$ iff $\langle \nabla \rangle_{nf} \supseteq \langle \nabla' \rangle_{nf}$.

$$
\left(\bigwedge_{a \not\# t \in \langle \nabla \rangle_{nf}} a \# NT[\![\varphi(t)]\!] \right) \quad \text{implies} \quad \left(\bigwedge_{a \not\# t \in \langle \nabla' \rangle_{nf}} a \# NT[\![\varphi(t)]\!] \right)
$$

Let $p \longrightarrow (\ell, p')$, $b \in \mathrm{bn}(\ell)$ and $c\#(\ell, p')$.

By equivariance of $\longrightarrow$ then $(b\,c) \cdot p \longrightarrow ((b\,c) \cdot \ell, (b\,c) \cdot p')$.

If $b\#p$ and $c\#p$ then $p \longrightarrow ((b\,c) \cdot \ell, (b\,c) \cdot p')$ as required by ACR property.

Let $p \longrightarrow (\ell, p')$, $b \in \mathrm{bn}(\ell)$ and $c\#(\ell, p')$.

By equivariance of $\longrightarrow$ then $(b\,c) \cdot p \longrightarrow ((b\,c) \cdot \ell, (b\,c) \cdot p')$.

If $b\#p$ and $c\#p$ then $p \longrightarrow ((b\,c) \cdot \ell, (b\,c) \cdot p')$ as required by ACR property.

Alpha-conversion-of-residuals format (ACR format)

For each rule

$$\frac{\{u_i \longrightarrow (\ell_i, u_i') \mid i \in I\} \qquad \nabla}{t \longrightarrow (\ell, t')}\ \mathsf{Ru}$$

such that $b \in \mathrm{bn}(\ell)$ check that

(i) $\nabla \cup \{b \not\approx u_i \mid i \in I \wedge b \in \mathrm{bn}(\ell_i)\} \vdash \{b \not\approx t\}$.

Let $p \longrightarrow (\ell, p')$, $b \in \mathrm{bn}(\ell)$ and $c\#(\ell, p')$.

By equivariance of $\longrightarrow$ then $(b\,c) \cdot p \longrightarrow ((b\,c) \cdot \ell, (b\,c) \cdot p')$.

If $b\#p$ and $c\#p$ then $p \longrightarrow ((b\,c) \cdot \ell, (b\,c) \cdot p')$ as required by ACR property.

Alpha-conversion-of-residuals format (ACR format)

For each rule

$$\frac{\{u_i \longrightarrow (\ell_i, u_i') \mid i \in I\} \qquad \nabla}{t \longrightarrow (\ell, t')}\ \mathsf{Ru}$$

such that $b \in \mathrm{bn}(\ell)$ check that

(i) $\nabla \cup \{b \not\approx u_i \mid i \in I \wedge b \in \mathrm{bn}(\ell_i)\} \vdash \{b \not\approx t\}$.

(ii) $\{a \not\approx t'\} \cup \nabla \vdash \{a \not\approx u_i' \mid i \in I\}$, and

(iii) $\{a \not\approx t'\} \cup \nabla \cup \{a \not\approx u_i \mid i \in I\} \vdash \{a \not\approx t\}$.

Let $p \longrightarrow (\ell, p')$, $b \in \mathrm{bn}(\ell)$ and $c\#(\ell, p')$.

By equivariance of $\longrightarrow$ then $(b\,c) \cdot p \longrightarrow ((b\,c) \cdot \ell, (b\,c) \cdot p')$.

If $b\#p$ and $c\#p$ then $p \longrightarrow ((b\,c) \cdot \ell, (b\,c) \cdot p')$ as required by ACR property.

Alpha-conversion-of-residuals format (ACR format)

For each rule

$$\frac{\{u_i \longrightarrow (\ell_i, u_i') \mid i \in I\} \qquad \nabla}{t \longrightarrow (\ell, t')}\ \mathsf{Ru}$$

such that $b \in \mathrm{bn}(\ell)$ check that

(i) $\nabla \cup \{b \not\approx u_i \mid i \in I \wedge b \in \mathrm{bn}(\ell_i)\} \vdash \{b \not\approx t\}$.

(ii) $\{a \not\approx t'\} \cup \nabla \vdash \{a \not\approx u_i' \mid i \in I\}$, and

(iii) $\{a \not\approx t'\} \cup \nabla \cup \{a \not\approx u_i \mid i \in I\} \vdash \{a \not\approx t\}$.

The ACR format also requires the equivariant format.

Theorem

If $\mathcal{R}$ is in ACR format with respect to bn, then the transition system induced by $\mathcal{R}$ together with bn constitute an NTS.

Conclusions

- Framework for SOS of languages with binding operations which stems from [Urban et al., 2004, Clouston and Pitts, 2007, Fernández and Gabbay, 2007, Cimini et al., 2012, Pitts, 2013]:
  - Raw terms (not up to alpha-equivalence) for specifications.
  - Nominal terms (up to alpha-equivalence) for proof trees.
- ACR format, which ensures that a specification system together with a function bn induces an NTS of [Parrow et al., 2015].

Conclusions

- Framework for SOS of languages with binding operations which stems from [Urban et al., 2004, Clouston and Pitts, 2007, Fernández and Gabbay, 2007, Cimini et al., 2012, Pitts, 2013]:
  - Raw terms (not up to alpha-equivalence) for specifications.
  - Nominal terms (up to alpha-equivalence) for proof trees.
- ACR format, which ensures that a specification system together with a function bn induces an NTS of [Parrow et al., 2015].

Future work

- Residuals of abstraction sort?

$$\begin{array}{rrcl} & \longrightarrow & : & \mathsf{pr} \to [\mathsf{ch}](\mathsf{ac} \times \mathsf{pr}) \\ \text{instead of} & \longrightarrow & : & \mathsf{pr} \to (\mathsf{ac} \times \mathsf{pr}) \text{ together with ACR property.} \end{array}$$

- Rule formats for congruence, bounded nondeterminism, . . . ?

Conclusions

- Framework for SOS of languages with binding operations which stems from [Urban et al., 2004, Clouston and Pitts, 2007, Fernández and Gabbay, 2007, Cimini et al., 2012, Pitts, 2013]:
  - Raw terms (not up to alpha-equivalence) for specifications.
  - Nominal terms (up to alpha-equivalence) for proof trees.
- ACR format, which ensures that a specification system together with a function bn induces an NTS of [Parrow et al., 2015].

Future work

- Residuals of abstraction sort?

$$\begin{array}{rrcl} & \longrightarrow & : & \mathsf{pr} \to [\mathsf{ch}](\mathsf{ac} \times \mathsf{pr}) \\ \text{instead of} & \longrightarrow & : & \mathsf{pr} \to (\mathsf{ac} \times \mathsf{pr}) \text{ together with ACR property.} \end{array}$$

- Rule formats for congruence, bounded nondeterminism, . . . ?

Thanks!

References I


Cimini, M., Mousavi, M. R., Reniers, M. A., and Gabbay, M. J. (2012).
Nominal SOS.
Electronic Notes in Theoretical Computer Science, 286:103–116.


Clouston, R. and Pitts, A. (2007).
Nominal equational logic.
Electronic Notes in Theoretical Computer Science, 172:223–257.


Fernández, M. and Gabbay, M. J. (2007).
Nominal rewriting.
Information and Computation, 205(6):917–965.


Parrow, J., Borgström, J., Eriksson, L.-H., Gutkovas, R., and Weber, T. (2015).
Modal logics for nominal transition systems.
In *26th International Conference on Concurrency Theory*, volume 42 of *LIPIcs*, pages 198–211. Schloss Dagstuhl.

References II


Pitts, A. (2013).
Nominal Sets: Names and Symmetry in Computer Science.
Cambridge University Press.


Urban, C., Pitts, A., and Gabbay, M. J. (2004).
Nominal unification.
Theoretical Computer Science, 323(1–3):473–497.

$$\frac{x \longrightarrow (outA(a,b), y) \qquad b \not\approx a}{new([b]x) \longrightarrow (boutA(a,b), y)}\ (\text{Open})$$

- $\{b \not\approx a\} \vdash \{b \not\approx new([b]x)\}$,

$$\frac{x \longrightarrow (outA(a,b),y) \qquad b \not\approx a}{new([b]x) \longrightarrow (boutA(a,b),y)}\ (\text{Open})$$

- $\{\ \} \vdash \{b \not\approx new([b]x)\}$,

$$\frac{x \longrightarrow (outA(a,b),y) \qquad b \not\approx a}{new([b]x) \longrightarrow (boutA(a,b),y)}\ (\text{Open})$$

- $\{\ \} \vdash \{b \not\approx [b]x\}$,

$$\frac{x \longrightarrow (outA(a,b), y) \qquad b \not\approx a}{new([b]x) \longrightarrow (boutA(a,b), y)}\ (\text{Open})$$

- $\{\ \} \vdash \{\ \}$,

$$\frac{x \longrightarrow (outA(a,b),y) \qquad b \not\approx a}{new([b]x) \longrightarrow (boutA(a,b),y)}\ (\text{Open})$$

- $\{\ \} \supseteq \{\ \}$,

$$\frac{x \longrightarrow (outA(a,b),y) \qquad b \not\approx a}{new([b]x) \longrightarrow (boutA(a,b),y)}\ (\text{Open})$$

- $\{\ \} \supseteq \{\ \}$,
- $\{c \not\approx (boutA(a,b),y), b \not\approx a\} \vdash \{c \not\approx (outA(a,b),y)\}$,

$$\frac{x \longrightarrow (outA(a,b), y) \qquad b \not\approx a}{new([b]x) \longrightarrow (boutA(a,b), y)}\ (\text{Open})$$

- $\{\ \} \supseteq \{\ \}$,
- $\{c \not\approx y\} \vdash \{c \not\approx y\}$,

$$\frac{x \longrightarrow (outA(a,b),y) \qquad b \not\approx a}{new([b]x) \longrightarrow (boutA(a,b),y)}\ (\text{Open})$$

- $\{\ \} \supseteq \{\ \}$,
- $\{c \not\approx y\} \supseteq \{c \not\approx y\}$,

$$\frac{x \longrightarrow (outA(a,b), y) \qquad b \not\approx a}{new([b]x) \longrightarrow (boutA(a,b), y)}\ (\text{Open})$$

- $\{\ \} \supseteq \{\ \}$,
- $\{c \not\approx y\} \supseteq \{c \not\approx y\}$, and
- $\{c \not\approx x\} \vdash \{c \not\approx new([b]x)\}$.

$$\frac{x \longrightarrow (outA(a,b), y) \qquad b \not\approx a}{new([b]x) \longrightarrow (boutA(a,b), y)}\ (\text{Open})$$

- $\{\ \} \supseteq \{\ \}$,
- $\{c \not\approx y\} \supseteq \{c \not\approx y\}$, and
- $\{c \not\approx x\} \vdash \{c \not\approx x\}$.

$$\frac{x \longrightarrow (outA(a,b), y) \qquad b \not\approx a}{new([b]x) \longrightarrow (boutA(a,b), y)}\ (\text{Open})$$

- $\{\ \} \supseteq \{\ \}$,
- $\{c \not\approx y\} \supseteq \{c \not\approx y\}$, and
- $\{c \not\approx x\} \supseteq \{c \not\approx x\}$.

Nominal Sets

- Countably infinite set of atoms $a, b, \ldots \in \mathbb{A}$.
- Finite permutations of atoms, $\pi \in \mathrm{Perm}\ \mathbb{A}$.
  $\pi = (a_1\ b_1) \circ \ldots \circ (a_k\ b_k)$ with finite $k \geq 0$.
- A $\mathrm{Perm}\ \mathbb{A}$-*set* S is a set equiped with a permutation action $\pi \cdot s$ for each $\pi \in \mathrm{Perm}\ \mathbb{A}$ and $s \in S$.
- Identity $\iota \cdot s = s$ and composition $\pi_1 \cdot (\pi_2 \cdot s) = (\pi_1 \circ \pi_2) \cdot s$ laws.
- The set of permutations is itself a $\mathrm{Perm}\ \mathbb{A}$-set where $\pi \cdot \pi_1 = \pi \circ \pi_1 \circ \pi^{-1}$.
- The set of functions of $\mathrm{Perm}\ \mathbb{A}$-sets is a $\mathrm{Perm}\ \mathbb{A}$-set where $(\pi \cdot f)(x) = \pi \cdot f(\pi^{-1} \cdot x)$.
- A set of atoms A *supports* an element $s \in S$ iff $\pi \cdot s = s$ for each π such that $\pi \cdot a = a$ for each $a \in A$.
- The *support* $\mathrm{supp}(s)$ of an element is the least set of atoms that supports s, if that set exists.
- An atom a *is fresh in* $s \in S$, written $a\#s$, iff $a \notin \mathrm{supp}(s)$.
- A *nominal set* S is a $\mathrm{Perm}\ \mathbb{A}$-set whose elements have finite support.

Nominal Sets

- Countably infinite set of atoms $a, b, \ldots \in \mathbb{A}$.
- Finite permutations of atoms, $\pi \in \mathrm{Perm}\ \mathbb{A}$.
  $\pi = (a_1\ b_1) \circ \ldots \circ (a_k\ b_k)$ with finite $k \geq 0$.
- A $\mathrm{Perm}\ \mathbb{A}$-*set* S is a set equiped with a permutation action $\pi \cdot s$ for each $\pi \in \mathrm{Perm}\ \mathbb{A}$ and $s \in S$.
- Identity $\iota \cdot s = s$ and composition $\pi_1 \cdot (\pi_2 \cdot s) = (\pi_1 \circ \pi_2) \cdot s$ laws.
- The set of permutations is itself a $\mathrm{Perm}\ \mathbb{A}$-set where $\pi \cdot \pi_1 = \pi \circ \pi_1 \circ \pi^{-1}$.
- The set of functions of $\mathrm{Perm}\ \mathbb{A}$-sets is a $\mathrm{Perm}\ \mathbb{A}$-set where $(\pi \cdot f)(x) = \pi \cdot f(\pi^{-1} \cdot x)$.
- A set of atoms A *supports* an element $s \in S$ iff $\pi \cdot s = s$ for each π such that $\pi \cdot a = a$ for each $a \in A$.
- The *support* $\mathrm{supp}(s)$ of an element is the least set of atoms that supports s, if that set exists.
- An atom a *is fresh in* $s \in S$, written $a\#s$, iff $a \notin \mathrm{supp}(s)$.
- A *nominal set* S is a $\mathrm{Perm}\ \mathbb{A}$-set whose elements have finite support.

Usual set constructions (products, unions, functions, power sets...) can be lifted to nominal sets by restricting them to elements with finite support. We write $\{S\}_{\mathrm{fs}}$ and $S \to_{\mathrm{fs}} T = \{S \to T\}_{\mathrm{fs}}$.

Nominal Sets

Definition (Equivariant function)

A nominal function $f : S \to_{\mathrm{fs}} T$ is *equivariant* if $\pi \cdot f(s) = f(\pi \cdot s)$ for every $\pi \in \mathrm{Perm}\ \mathbb{A}$ and $s \in S$.

Nominal Sets

Definition (Equivariant function)

A nominal function $f : S \to_{\mathrm{fs}} T$ is *equivariant* if $\pi \cdot f(s) = f(\pi \cdot s)$ for every $\pi \in \mathrm{Perm}\ \mathbb{A}$ and $s \in S$.

Intuition: f is equivariant iff $\mathrm{supp}(f) = \emptyset$, i.e., f does not treat any atom preferentially.

Nominal Sets

Definition (Equivariant function)

A nominal function $f : S \to_{\mathrm{fs}} T$ is *equivariant* if $\pi \cdot f(s) = f(\pi \cdot s)$ for every $\pi \in \mathrm{Perm}\ \mathbb{A}$ and $s \in S$.

Intuition: f is equivariant iff $\mathrm{supp}(f) = \emptyset$, i.e., f does not treat any atom preferentially.

Definition (Atom abstraction)

The *atom abstraction* $\langle a \rangle s$ of atom a in element s is the $\mathrm{Perm}\ \mathbb{A}$-set $\{(b, (b\,a) \cdot s) \mid b = a \vee b \# s\}$.
We write $[\mathbb{A}]S$ for the *set of atom abstractions* of atoms $a \in \mathbb{A}$ in elements $s \in S$.

$$\begin{array}{rcl} \pi \cdot \langle a \rangle s & = & \langle \pi \cdot a \rangle (\pi \cdot s) \\ \mathrm{supp}(\langle a \rangle s) & = & \mathrm{supp}(s) \setminus \{a\}. \end{array}$$

Nominal Sets

Definition (Equivariant function)

A nominal function $f : S \to_{\mathrm{fs}} T$ is *equivariant* if $\pi \cdot f(s) = f(\pi \cdot s)$ for every $\pi \in \mathrm{Perm}\ \mathbb{A}$ and $s \in S$.

Intuition: f is equivariant iff $\mathrm{supp}(f) = \emptyset$, i.e., f does not treat any atom preferentially.

Definition (Atom abstraction)

The *atom abstraction* $\langle a \rangle s$ of atom a in element s is the $\mathrm{Perm}\ \mathbb{A}$-set $\{(b, (b\,a) \cdot s) \mid b = a \vee b \# s\}$.
We write $[\mathbb{A}]S$ for the *set of atom abstractions* of atoms $a \in \mathbb{A}$ in elements $s \in S$.

$$\begin{array}{rcl} \pi \cdot \langle a \rangle s & = & \langle \pi \cdot a \rangle (\pi \cdot s) \\ \mathrm{supp}(\langle a \rangle s) & = & \mathrm{supp}(s) \setminus \{a\}. \end{array}$$

Intuition: the set of atom abstractions provides inductive principles to deal with alpha-equivalence classes.

$$(\mathbb{A} \times S)/_{=_\alpha} \cong [\mathbb{A}]S.$$

Sorts and Signatures

- Sorted atoms:

$$\mathbb{A} = \sum_{\alpha \in A} \mathbb{A}_\alpha \quad \text{with } A = \{\alpha_1, \alpha_2, \ldots\} \text{ countable set of atom sorts.}$$

- Sort-preserving permutations:

$$\mathrm{Perm}_s\, \mathbb{A} = \{\pi \in \mathrm{Perm}\ \mathbb{A} \mid \forall \alpha \in A.\, \forall a \in \mathbb{A}_\alpha.\, \pi\, a \in \mathbb{A}_\alpha\}.$$

- Nominal signature: $\Sigma = (\Delta, A, F)$

$$\begin{array}{rcl} \Delta & = & \{\delta_1, \ldots, \delta_n\} \text{ finite set of base sorts,} \\ A & = & \{\alpha_1, \alpha_2, \ldots\} \text{ countable set of atom sorts, and} \\ F & = & \{f_{11} : \sigma_{11} \to \delta_1, \ldots, f_{1m_1} : \sigma_{1m_1} \to \delta_1, \\ & & \qquad \ldots, \\ & & f_{n1} : \sigma_{n1} \to \delta_n, \ldots, f_{nm_n} : \sigma_{nm_n} \to \delta_n\} \\ & & \text{finite set of function symbols.} \end{array}$$

- Nominal sorts:

$$\sigma ::= \delta \mid \alpha \mid [\alpha]\sigma \mid \sigma_1 \times \ldots \times \sigma_k \quad \text{where } \alpha \in A \text{ and } \delta \in \Delta.$$

Raw Terms

- Variables:

$$\mathcal{V} = \sum_{\sigma \in \mathsf{S}} \mathcal{V}_\sigma \quad \text{with S the set of nominal sorts.}$$

- Raw terms:

$$t_\sigma ::= x_\sigma \mid a_\alpha \mid (\pi \bullet t_\sigma)_\sigma \mid ([a_\alpha]t_\sigma)_{[\alpha]\sigma} \mid (t_{\sigma_1}, \ldots, t_{\sigma_k})_{\sigma_1 \times \ldots \times \sigma_k} \mid (f_{ij}(t_{\sigma_{ij}}))_{\delta_i}$$

with $x_\sigma \in \mathcal{V}_\sigma$, $a_\alpha \in \mathbb{A}_\alpha$, $\pi \in \mathrm{Perm}_s\, \mathbb{A}$, and $f_{ij} \in F$.

Definition (Raw terms)

The indexed family $\mathbb{T}(\Sigma, \mathcal{V})_\sigma$ of *raw terms* is the sorted free algebra over the set of variables $\mathcal{V}$ and function symbols

$$\begin{aligned} & F \cup \{a_\alpha : \alpha \mid \alpha \in A\} \cup \\ & \quad \{(\pi \bullet \_)_\sigma : \sigma \to \sigma \mid \pi \in \mathrm{Perm}_s\, \mathbb{A} \wedge \sigma \in \mathsf{S}\} \cup \\ & \quad \{([a_\alpha]\_)_{[\alpha]\sigma} : \sigma \to [\alpha]\sigma \mid a_\alpha \in \mathbb{A}_\alpha \wedge \sigma \in \mathsf{S}\} \cup \\ & \quad \{(\_, \ldots, \_)_{\sigma_1 \times \ldots \times \sigma_k} : \sigma_1 \times \ldots \times \sigma_k \to \sigma_1 \times \ldots \times \sigma_k \mid \sigma_1, \ldots \sigma_k \in \mathsf{S}\}. \end{aligned}$$

We elide sorts and arities and write x, a, $\pi \bullet t$, $[a]t$, $(t_1 \ldots, t_k)$, $f(t)$, ...

Raw Terms

The set of raw terms is a nominal set, where

$$
\begin{array}{rcl}
\pi \cdot x & = & x \\
\pi \cdot a & = & \pi\, a \\
\pi \cdot (\pi_1 \bullet t) & = & (\pi \cdot \pi_1) \bullet (\pi \cdot t) \\
\pi \cdot [a]t & = & [\pi\, a](\pi \cdot t) \\
\pi \cdot (t_1, \ldots, t_k) & = & (\pi \cdot t_1, \ldots, \pi \cdot t_k) \\
\pi \cdot (f(t)) & = & f(\pi \cdot t),
\end{array}
$$

$$
\begin{array}{rcl}
\mathrm{supp}(x) & = & \emptyset \\
\mathrm{supp}(a) & = & \{a\} \\
\mathrm{supp}(\pi \bullet t) & = & \mathrm{supp}(\pi) \cup \mathrm{supp}(t) \\
\mathrm{supp}([a]t) & = & \{a\} \cup \mathrm{supp}(t) \\
\mathrm{supp}((t_1, \ldots, t_k)) & = & \mathrm{supp}(t_1) \cup \ldots \cup \mathrm{supp}(t_k) \\
\mathrm{supp}(f(t)) & = & \mathrm{supp}(t).
\end{array}
$$

Substitution

Definition (Substitution)

Sort-preserving, finitely supported nominal function $\varphi : \mathcal{V} \to_{\mathrm{fs}} \mathbb{T}(\Sigma, \mathcal{V})$ from variables to raw terms.
The *domain* of φ is $\mathrm{dom}(\varphi) = \{x \in \mathcal{V} \mid \varphi(x) \neq x\}$.

Extension to raw terms $\overline{\varphi}$ of substitution φ: unique homomorphism induced by φ from the free algebra $\mathbb{T}(\Sigma, \mathcal{V})$ to itself, which coincides with the nominal function $\overline{\varphi} : \mathbb{T}(\Sigma, \mathcal{V}) \to_{\mathrm{fs}} \mathbb{T}(\Sigma, \mathcal{V})$ defined as

$$\begin{aligned}
\overline{\varphi}(x) &= \varphi(x) \\
\overline{\varphi}(a) &= a \\
\overline{\varphi}(\pi \bullet t) &= \pi \bullet \overline{\varphi}(t) \\
\overline{\varphi}([a]t) &= [a](\overline{\varphi}(t)) \\
\overline{\varphi}(t_1, \ldots, t_k) &= (\overline{\varphi}(t_1), \ldots, \overline{\varphi}(t_k)) \\
\overline{\varphi}(f(t)) &= f(\overline{\varphi}(t)).
\end{aligned}$$

Substitution

Lemma

Extension to raw terms is equivariant, i.e., $(\pi \cdot \overline{\varphi})(t) = \overline{\pi \cdot \varphi}(t)$.

We write $\varphi(t)$ instead of $\overline{\varphi}(t)$ and $\varphi^{\pi}(t)$ instead of $\overline{\pi \cdot \varphi}(t)$.

Lemma

The action of substitution is equivariant, i.e., $\pi \cdot \varphi(t) = \varphi^{\pi}(\pi \cdot t)$.

Ground Terms

A ground term p is a raw term without occurrences of variables.

Definition (Ground terms)

The indexed family $\mathbb{T}(\Sigma)_\sigma$ of *ground terms* is the sorted term algebra over the function symbols

$$
\begin{aligned}
&F \cup \{a_\alpha : \alpha \mid \alpha \in A\} \cup \\
&\quad \{(\pi \bullet \_)_\sigma : \sigma \to \sigma \mid \pi \in \mathrm{Perm}_s\, \mathbb{A} \wedge \sigma \in \mathsf{S}\} \cup \\
&\quad \{([a_\alpha]\_)_{[\alpha]\sigma} : \sigma \to [\alpha]\sigma \mid a_\alpha \in \mathbb{A}_\alpha \wedge \sigma \in \mathsf{S}\} \cup \\
&\quad \{(\_, \ldots, \_)_{\sigma_1 \times \ldots \times \sigma_k} : \sigma_1 \times \ldots \times \sigma_k \to \sigma_1 \times \ldots \times \sigma_k \mid \sigma_1, \ldots \sigma_k \in \mathsf{S}\}.
\end{aligned}
$$

Ground Terms

A ground term p is a raw term without occurrences of variables.

Definition (Ground terms)

The indexed family $\mathbb{T}(\Sigma)_\sigma$ of *ground terms* is the sorted term algebra over the function symbols

$$
\begin{aligned}
&F \cup \{a_\alpha : \alpha \mid \alpha \in A\} \cup \\
&\quad \{(\pi \bullet \_)_\sigma : \sigma \to \sigma \mid \pi \in \mathrm{Perm}_s\, \mathbb{A} \wedge \sigma \in \mathsf{S}\} \cup \\
&\quad \{([a_\alpha]\_)_{[\alpha]\sigma} : \sigma \to [\alpha]\sigma \mid a_\alpha \in \mathbb{A}_\alpha \wedge \sigma \in \mathsf{S}\} \cup \\
&\quad \{(\_, \ldots, \_)_{\sigma_1 \times \ldots \times \sigma_k} : \sigma_1 \times \ldots \times \sigma_k \to \sigma_1 \times \ldots \times \sigma_k \mid \sigma_1, \ldots \sigma_k \in \mathsf{S}\}.
\end{aligned}
$$

A substitution φ is *ground* iff $\varphi(x) \in \mathbb{T}(\Sigma)$ for every $x \in \mathrm{dom}(\varphi)$.

Interpretation

Definition (Σ-structure)

Let Σ be a nominal signature. A Σ-*structure* consists of

- a nominal set $M[\![\sigma]\!]$ for each sort $\sigma \in \mathsf{S}$ defined as

$$\begin{aligned} M[\![\alpha]\!] &= \mathbb{A}_\alpha \\ M[\![[\alpha]\sigma]\!] &= [\mathbb{A}_\alpha](M[\![\sigma]\!]) \\ M[\![\sigma_1 \times \ldots \times \sigma_k]\!] &= M[\![\sigma_1]\!] \times \ldots \times M[\![\sigma_k]\!] \end{aligned}$$

  where the tuple $(M[\![\delta_1]\!], \ldots, M[\![\delta_n]\!])$ of sets of base sort is given, and
- an equivariant function $M[\![f_{ij}]\!] : M[\![\sigma_{ij}]\!] \to M[\![\delta_i]\!]$ for each symbol $f_{ij} : \sigma_{ij} \to \delta_i \in F$.

The *interpretation* $M[\![p]\!]$ of a ground term p in the Σ-structure M is

$$\begin{aligned} M[\![a]\!] &= a \\ M[\![\pi \bullet p]\!] &= \pi \cdot M[\![p]\!] \\ M[\![[a]p]\!] &= \langle a \rangle (M[\![p]\!]) \\ M[\![(p_1, \ldots, p_k)]\!] &= (M[\![p_1]\!], \ldots, M[\![p_k]\!]) \\ M[\![f(p)]\!] &= M[\![f]\!](M[\![p]\!]). \end{aligned}$$

Nominal Terms

Definition (Σ-structure for nominal terms)

The Σ-structure NT for nominal terms is given by

- the least tuple $(NT[\![\delta_1]\!], \ldots, NT[\![\delta_n]\!])$ satisfying

$$NT[\![\delta_i]\!] = NT[\![\sigma_{i1}]\!] + \ldots + NT[\![\sigma_{im_i}]\!] \text{ for each base sort } \delta_i, \text{ and}$$

- the equivariant functions $NT[\![f_{ij}]\!] = \mathrm{inj}_j : NT[\![\sigma_{ij}]\!] \to NT[\![\delta_i]\!]$ for each function symbol $f_{ij} \in F$.
  (Recall, $\mathrm{inj}_j : S_j \to S_1 + \ldots + S_j + \ldots S_n$.)

Definition (Nominal terms)

The indexed family $\mathbb{N}(\Sigma)_\sigma$ of *nominal terms* is the interpretation of the indexed family $\mathbb{T}(\Sigma)_\sigma$ of ground terms in the Σ-structure NT, i.e., $\mathbb{N}(\Sigma)_\sigma = NT[\![\sigma]\!]$.

Lemma

The nominal sets $\mathbb{N}(\Sigma)_\sigma$ coincide with the nominal algebraic datatypes of Definition 8.9 in [Pitts, 2013].

Example (π-Calculus)

Nominal signature Σ with base sorts $\Delta = \{\mathsf{pr}, \mathsf{ac}\}$, atom sorts $A = \{\mathsf{ch}\}$ and function symbols

$$
\begin{aligned}
F = \{\ & \mathit{null} : \mathbf{1} \to \mathsf{pr}, \\
& \mathit{tau} : \mathsf{pr} \to \mathsf{pr}, \\
& \mathit{in} : (\mathsf{ch} \times [\mathsf{ch}]\mathsf{pr}) \to \mathsf{pr}, \\
& \mathit{out} : (\mathsf{ch} \times \mathsf{ch} \times \mathsf{pr}) \to \mathsf{pr}, \\
& \mathit{par} : (\mathsf{pr} \times \mathsf{pr}) \to \mathsf{pr}, \\
& \mathit{sum} : (\mathsf{pr} \times \mathsf{pr}) \to \mathsf{pr}, \\
& \mathit{rep} : \mathsf{pr} \to \mathsf{pr}, \\
& \mathit{new} : [\mathsf{ch}]\mathsf{pr} \to \mathsf{pr}, \\
& \mathit{tauA} : \mathbf{1} \to \mathsf{ac}, \\
& \mathit{inA} : (\mathsf{ch} \times \mathsf{ch}) \to \mathsf{ac}, \\
& \mathit{outA} : (\mathsf{ch} \times \mathsf{ch}) \to \mathsf{ac}, \\
& \mathit{boutA} : (\mathsf{ch} \times \mathsf{ch}) \to \mathsf{ac} \quad \}.
\end{aligned}
$$

$$
NT[\![\mathit{new}([b](\mathit{out}(a, b, p)))]\!] \longrightarrow NT[\![(\mathit{boutA}(a, b), p)]\!]
$$

stands for the residual notation of $(\nu b)(\overline{a}b.p) \xrightarrow{\overline{a}(\nu b)} p$

Nominal Residual Transition System (NRTS)

- Nominal residual signature: $\Sigma = (\Delta, A, \sigma, \rho, F)$ where (Δ, A, F) is a nominal signature and $\sigma \in \mathsf{S}$ is a distinguished sort of *states* and $\rho \in \mathsf{S}$ is a distinguished sort of *residuals*.

Definition (Nominal residual transition system (NRTS))

Triple $(S, R, \longrightarrow)$ where

(i) S and R are nominal sets of *states* and *residuals* respectively, and

(ii) $\longrightarrow \subseteq S \times R$ is an equivariant binary *transition relation*.

Let $\mathcal{T}$ be an NRTS and Σ be a nominal residual signature. We say $\mathcal{T}$ is over Σ iff $S = \mathbb{N}(\Sigma)_\sigma$ and $R = \mathbb{N}(\Sigma)_\rho$.

Nominal Residual Transition System Specification (NRTSS)

- Transition formula: $s \longrightarrow r$ where $s \in \mathbb{T}(\Sigma, \mathcal{V})_\sigma$ and $r \in \mathbb{T}(\Sigma, \mathcal{V})_\rho$.
- Freshness assertion: $a \not\approx t$ where $a \in \mathbb{A}$ and $t \in \mathbb{T}(\Sigma, \mathcal{V})$.

Definition (Nominal residual transition system spec. (NRTSS))

Let Σ be a nominal residual signature. An NRTSS over Σ is a set of rules

$$\frac{\{u_i \longrightarrow u_i' \mid i \in I\} \quad \{a_j \not\approx v_j \mid j \in J\}}{t \longrightarrow t'}\ \text{Ru}$$

where $H = \{u_i \longrightarrow u_i' \mid i \in I\}$ is a finitely supported set of transition formulas and $\nabla = \{a_j \not\approx v_j \mid j \in J\}$ is a finite set of freshness assertions.

Nominal Residual Transition System Specification (NRTSS)

- Transition formula: $s \longrightarrow r$ where $s \in \mathbb{T}(\Sigma, \mathcal{V})_\sigma$ and $r \in \mathbb{T}(\Sigma, \mathcal{V})_\rho$.
- Freshness assertion: $a \not\# t$ where $a \in \mathbb{A}$ and $t \in \mathbb{T}(\Sigma, \mathcal{V})$.

Definition (Nominal residual transition system spec. (NRTSS))

Let Σ be a nominal residual signature. An NRTSS over Σ is a set of rules

$$\frac{\{u_i \longrightarrow u_i' \mid i \in I\} \quad \{a_j \not\# v_j \mid j \in J\}}{t \longrightarrow t'}\ \mathrm{Ru}$$

where $H = \{u_i \longrightarrow u_i' \mid i \in I\}$ is a finitely supported set of transition formulas and $\nabla = \{a_j \not\# v_j \mid j \in J\}$ is a finite set of freshness assertions.

The permutation action can be lifted to rules, i.e., $\pi \cdot \mathrm{Ru}$, with $\mathrm{Ru} \in \mathcal{R}$.

Example (SOS for the π-Calculus)

$$\frac{d \not\approx x}{in(a,[b]x) \longrightarrow (inA(a,c),((d\ b)\cdot(b\ c)) \bullet x)}\ (\mathsf{In})$$

$$\frac{x \longrightarrow (outA(a,b),y) \qquad b \not\approx a}{new([b]x) \longrightarrow (boutA(a,b),y)}\ (\mathsf{Open})$$

$$\frac{}{out(a,b,x) \longrightarrow (outA(a,b),x)}\ (\mathsf{Out})$$

$$\frac{x_1 \longrightarrow (boutA(a,b),y_1) \qquad x_2 \longrightarrow (inA(a,b),y_2) \qquad b \not\approx x_2}{par(x_1,x_2) \longrightarrow (tauA, new([b](par(y_1,y_2))))}\ (\mathsf{CloseL})$$

Proof Tree

Let $\mathcal{R}$ be an NRTSS over Σ, and let $NT[\![s]\!] \longrightarrow NT[\![r]\!]$ be a transition where $NT[\![s]\!] \in \mathbb{N}(\Sigma)_\sigma$ and $NT[\![r]\!] \in \mathbb{N}(\Sigma)_\rho$.

Definition (Proof tree of $NT[\![s]\!] \longrightarrow NT[\![r]\!]$ in $\mathcal{R}$)

A proof tree of $NT[\![s]\!] \longrightarrow NT[\![r]\!]$ in $\mathcal{R}$ is a tree without infinite paths whose nodes are transitions such that

(i) the root is $NT[\![s]\!] \longrightarrow NT[\![r]\!]$, and

(ii) if $\{NT[\![q_i]\!] \longrightarrow NT[\![q_i']\!] \mid i \in I\}$ is the set of nodes above a node $NT[\![p]\!] \longrightarrow NT[\![p']\!]$, then $\mathcal{R}$ contains a rule

$$\frac{\{u_i \longrightarrow u_i' \mid i \in I\} \quad \{a_j \not\approx v_j \mid j \in J\}}{t \longrightarrow t'}\ \text{Ru}$$

and there exists a ground substitution φ such that

- $\varphi(t) \longrightarrow \varphi(t') = p \longrightarrow p'$,
- $\varphi(u_i) \longrightarrow \varphi(u_i') = u_i \longrightarrow q_i'$ for each $i \in I$, and
- $a_j \# NT[\![\varphi(v_j)]\!]$ holds for each $j \in J$.

Example (Transition up to Alpha-Equivalence)

$$\dfrac{\dfrac{}{NT[\![out(a,b,p)]\!] \longrightarrow NT[\![(outA(a,b),p)]\!]}\ (\mathsf{Out},\varphi_1)}{NT[\![new([b](out(a,b,p)))]\!] \longrightarrow NT[\![(boutA(a,b),p)]\!]}\ (\mathsf{Open},\varphi_2) \text{ and } b\#a$$

$$\dfrac{}{out(a,b,x) \longrightarrow (outA(a,b),x)}\ (\mathsf{Out}) \qquad \begin{array}{lcl} \varphi_1(x) & = & p \end{array}$$

$$\dfrac{x \longrightarrow (outA(a,b),y) \qquad b \not\# a}{new([b]x) \longrightarrow (boutA(a,b),y)}\ (\mathsf{Open}) \qquad \begin{array}{lcl} \varphi_2(x) & = & out(a,b,p) \\ \varphi_2(y) & = & p \end{array}$$

Example (Transition up to Alpha-Equivalence)

$$\dfrac{\dfrac{}{NT[\![out(a,b,p)]\!] \longrightarrow NT[\![(outA(a,b),p)]\!]}\ (\mathsf{Out},\varphi_1)}{NT[\![new([b](out(a,b,p)))]\!] \longrightarrow NT[\![(boutA(a,b),p)]\!]}\ (\mathsf{Open},\varphi_2) \text{ and } b\#a$$

$$\dfrac{}{out(a,b,x) \longrightarrow (outA(a,b),x)}\ (\mathsf{Out}) \qquad \begin{array}{lcl} \varphi_1(x) & = & p \end{array}$$

$$\dfrac{x \longrightarrow (outA(a,b),y) \qquad b \not\# a}{new([b]x) \longrightarrow (boutA(a,b),y)}\ (\mathsf{Open}) \qquad \begin{array}{lcl} \varphi_2(x) & = & out(a,b,p) \\ \varphi_2(y) & = & p \end{array}$$

$$NT[\![new([c](out(a,c,(b\,c)\cdot p)))]\!] \longrightarrow NT[\![(boutA(a,b),p)]\!] \quad \text{with } c\#p$$

has the same proof tree because

$$NT[\![new([c](out(a,c,(b\,c)\cdot p)))]\!] = NT[\![new([b](out(a,b,p)))]\!]$$

NRTSS induces an NRTS

An NRTSS induces a transition realtion. We need to ensure that the transition relation is equivariant.

Definition (Equivariant Format)

Let $\mathcal{R}$ be an NRTSS. $\mathcal{R}$ is in *equivariant format* iff for every rule $\mathsf{Ru} \in \mathcal{R}$ and every $\pi \in \mathrm{Perm}_s\, \mathbb{A}$, then $\pi \cdot \mathsf{Ru} \in \mathcal{R}$.

Theorem (Rule format for NRTSs)

Let $\mathcal{R}$ be an NRTSS in equivariant format, then the transition relation induced by $\mathcal{R}$ is equivariant.

If $\mathcal{R}$ is in equivariant format, then $\mathcal{R}$ induces an NRTS.

Studying NTS in Terms of NRTS

An NTS of [Parrow et al., 2015] can be specified by using the nominal residual signature Σ_{NTS} with base sorts $\Delta = \{\mathsf{pr}, \mathsf{ac}\}$, atom sorts $A = \{\mathsf{ch}\}$, state sort $\sigma = \mathsf{pr}$, residual sort $\rho = (\mathsf{ac}, \mathsf{pr})$, and a given set of function symbols F.

Let $\mathcal{R}$ be an NRTSS over Σ_{NTS}. If $\mathcal{R}$ is in equivariant format then $\mathcal{R}$ induces an NRTS $\mathcal{T}$ over signature Σ_{NTS}.

Furthermore, if $\mathcal{T}$ satisfies alpha-conversion of residuals, then $\mathcal{T}$ is an NTS.

Simplification of Freshness Environments ∇

Adapted from [Fernández and Gabbay, 2007].

Definition (Simplification relation for freshness environments)

$$
\begin{array}{rcl}
\{a \not\approx b\} \cup \nabla & \Longrightarrow & \nabla \\
\{a \not\approx \pi \bullet t\} \cup \nabla & \Longrightarrow & \{\pi^{-1} \cdot a \not\approx t\} \cup \nabla \\
\{a \not\approx [b]p\} \cup \nabla & \Longrightarrow & \{a \not\approx p\} \cup \nabla \\
\{a \not\approx [a]p\} \cup \nabla & \Longrightarrow & \nabla \\
\{a \not\approx f(p)\} \cup \nabla & \Longrightarrow & \{a \not\approx p\} \cup \nabla \\
\{a \not\approx (p_1, \ldots, p_k)\} \cup \nabla & \Longrightarrow & \{a \not\approx p_i, \ldots, a \not\approx p_k\} \cup \nabla.
\end{array}
$$

Lemma

The relation $\Longrightarrow$ is confluent and terminating.

Simplification of Freshness Environments ∇

Adapted from [Fernández and Gabbay, 2007].

Definition (Simplification relation for freshness environments)

$$
\begin{array}{rcl}
\{a \not\approx b\} \cup \nabla & \Longrightarrow & \nabla \\
\{a \not\approx \pi \bullet t\} \cup \nabla & \Longrightarrow & \{\pi^{-1} \cdot a \not\approx t\} \cup \nabla \\
\{a \not\approx [b]p\} \cup \nabla & \Longrightarrow & \{a \not\approx p\} \cup \nabla \\
\{a \not\approx [a]p\} \cup \nabla & \Longrightarrow & \nabla \\
\{a \not\approx f(p)\} \cup \nabla & \Longrightarrow & \{a \not\approx p\} \cup \nabla \\
\{a \not\approx (p_1, \ldots, p_k)\} \cup \nabla & \Longrightarrow & \{a \not\approx p_i, \ldots, a \not\approx p_k\} \cup \nabla.
\end{array}
$$

Lemma

The relation $\Longrightarrow$ is confluent and terminating.

Intuition: normal forms exist and are unique.

Simplification of Freshness Environments ∇

Adapted from [Fernández and Gabbay, 2007].

Definition (Simplification relation for freshness environments)

$$
\begin{array}{rcl}
\{a \not\approx b\} \cup \nabla & \Longrightarrow & \nabla \\
\{a \not\approx \pi \bullet t\} \cup \nabla & \Longrightarrow & \{\pi^{-1} \cdot a \not\approx t\} \cup \nabla \\
\{a \not\approx [b]p\} \cup \nabla & \Longrightarrow & \{a \not\approx p\} \cup \nabla \\
\{a \not\approx [a]p\} \cup \nabla & \Longrightarrow & \nabla \\
\{a \not\approx f(p)\} \cup \nabla & \Longrightarrow & \{a \not\approx p\} \cup \nabla \\
\{a \not\approx (p_1, \ldots, p_k)\} \cup \nabla & \Longrightarrow & \{a \not\approx p_i, \ldots, a \not\approx p_k\} \cup \nabla.
\end{array}
$$

Lemma

The relation $\Longrightarrow$ is confluent and terminating.

Intuition: normal forms exist and are unique.

We write $\langle \nabla \rangle_{nf}$ for the *normal form* of ∇.

Simplification of Freshness Environments ∇

- An environment ∇ is *inconsistent* iff $a \not\# a \in \langle \nabla \rangle_{nf}$ for some $a \in \mathbb{A}$.
- We say $\nabla \vdash \nabla'$ iff either ∇ is inconsistent or $\langle \nabla' \rangle_{nf} \subseteq \langle \nabla \rangle_{nf}$.
- We write $\vdash \nabla$ instead of $\emptyset \vdash \nabla$, this is, $\langle \nabla \rangle_{nf} = \emptyset$.

Lemma

Let ∇ be a freshness environment. For every ground substitution φ,

$$\left(\bigcap_{a \not\# t \in \nabla} a\#NT[\![\varphi(t)]\!] \right) \textit{ iff } \left(\bigcap_{a \not\# t \in \langle \nabla \rangle_{nf}} a\#NT[\![\varphi(t)]\!] \right).$$

Simplification of Freshness Environments ∇

- An environment ∇ is *inconsistent* iff $a \not\# a \in \langle \nabla \rangle_{nf}$ for some $a \in \mathbb{A}$.
- We say $\nabla \vdash \nabla'$ iff either ∇ is inconsistent or $\langle \nabla' \rangle_{nf} \subseteq \langle \nabla \rangle_{nf}$.
- We write $\vdash \nabla$ instead of $\emptyset \vdash \nabla$, this is, $\langle \nabla \rangle_{nf} = \emptyset$.

Lemma

Let ∇ be a freshness environment. For every ground substitution φ,

$$\left(\bigcap_{a \not\# t \in \nabla} a\#NT[\![\varphi(t)]\!] \right) \textit{ iff } \left(\bigcap_{a \not\# t \in \langle \nabla \rangle_{nf}} a\#NT[\![\varphi(t)]\!] \right).$$

Intuition: simplification commutes with the interpretation of $a \not\# t \in \nabla$ into $a\#NT[\![\varphi(t)]\!]$ for every ground substitution φ.

Simplification of Freshness Environments ∇

- An environment ∇ is *inconsistent* iff $a \not\# a \in \langle \nabla \rangle_{nf}$ for some $a \in \mathbb{A}$.
- We say $\nabla \vdash \nabla'$ iff either ∇ is inconsistent or $\langle \nabla' \rangle_{nf} \subseteq \langle \nabla \rangle_{nf}$.
- We write $\vdash \nabla$ instead of $\emptyset \vdash \nabla$, this is, $\langle \nabla \rangle_{nf} = \emptyset$.

Lemma

Let ∇ be a freshness environment. For every ground substitution φ,

$$\left(\bigcap_{a \not\# t \in \nabla} a\#NT[\![\varphi(t)]\!] \right) \textit{ iff } \left(\bigcap_{a \not\# t \in \langle \nabla \rangle_{nf}} a\#NT[\![\varphi(t)]\!] \right).$$

Intuition: simplification commutes with the interpretation of $a \not\# t \in \nabla$ into $a\#NT[\![\varphi(t)]\!]$ for every ground substitution φ.

In particular, if $\vdash \nabla$ then for every ground subsitution φ

$$\bigcap_{a \not\# t \in \nabla} a\#NT[\![\varphi(t)]\!].$$

Simplification of Freshness Environments ∇

- An environment ∇ is *inconsistent* iff $a \not\# a \in \langle \nabla \rangle_{nf}$ for some $a \in \mathbb{A}$.
- We say $\nabla \vdash \nabla'$ iff either ∇ is inconsistent or $\langle \nabla' \rangle_{nf} \subseteq \langle \nabla \rangle_{nf}$.
- We write $\vdash \nabla$ instead of $\emptyset \vdash \nabla$, this is, $\langle \nabla \rangle_{nf} = \emptyset$.

Lemma

Let ∇ be a freshness environment. For every ground substitution φ,

$$\left(\bigcap_{a \not\# t \in \nabla} a\#NT[\![\varphi(t)]\!] \right) \textit{ iff } \left(\bigcap_{a \not\# t \in \langle \nabla \rangle_{nf}} a\#NT[\![\varphi(t)]\!] \right).$$

Intuition: simplification commutes with the interpretation of $a \not\# t \in \nabla$ into $a\#NT[\![\varphi(t)]\!]$ for every ground substitution φ.

In particular, if $\vdash \nabla$ then for every ground subsitution φ

$$\bigcap_{a \not\# t \in \nabla} a\#NT[\![\varphi(t)]\!].$$

Intuition: if $\vdash \nabla$, then the interpretation of ∇'s assertions into freshness relations hold for every ground substitution φ.

Partial Strict Stratification

Definition (Partial strict stratification)

Let $\mathcal{R}$ be an NRTSS over Σ_{NTS} and bn be a binding-names function. S is a *partial strict stratification of $\mathcal{R}$ with respect to* bn iff

(i) $S(\varphi(t), \ell) \neq \bot$, for every rule in $\mathcal{R}$ with conclusion $t \longrightarrow (\ell, t')$ such that $bn(\ell)$ is non-empty, and for every ground substitution φ, and

(ii) $S(\varphi(u_i), \ell_i) < S(\varphi(t), \ell)$, for every rule in $\mathcal{R}$ with conclusion $t \longrightarrow (\ell, t')$ and for every premiss $u_i \longrightarrow (\ell_i, u_i')$ of $\mathcal{R}$, and for every ground substitution φ such that $S(\varphi(t), \ell) \neq \bot$ and $S(\varphi(u_i), \ell_i) \neq \bot$.

Partial Strict Stratification

Definition (Partial strict stratification)

Let $\mathcal{R}$ be an NRTSS over Σ_{NTS} and bn be a binding-names function. S is a *partial strict stratification of $\mathcal{R}$ with respect to* bn iff

(i) $S(\varphi(t), \ell) \neq \bot$, for every rule in $\mathcal{R}$ with conclusion $t \longrightarrow (\ell, t')$ such that $bn(\ell)$ is non-empty, and for every ground substitution φ, and

(ii) $S(\varphi(u_i), \ell_i) < S(\varphi(t), \ell)$, for every rule in $\mathcal{R}$ with conclusion $t \longrightarrow (\ell, t')$ and for every premiss $u_i \longrightarrow (\ell_i, u_i')$ of $\mathcal{R}$, and for every ground substitution φ such that $S(\varphi(t), \ell) \neq \bot$ and $S(\varphi(u_i), \ell_i) \neq \bot$.

Intuition: the rules with order $\neq \bot$ are those which can occur in a proof tree above a rule which enables transitions with binding names in their actions, and they occur in stratified fashion.

Example (Partial Strict Stratification for the π-Calculus)

$$
\begin{aligned}
S(out(a,b,p), outA(a,b)) &= 0 \\
S(par(p,q),\ell) &= 1 + \max\{S(p,\ell), S(q,\ell)\} \\
&\quad \text{if } \ell \in \{boutA(a,b), outA(a,b)\} \\
S(sum(p,q),\ell) &= 1 + \max\{S(p,\ell), S(q,\ell)\} \\
&\quad \text{if } \ell \in \{boutA(a,b), outA(a,b)\} \\
S(rep(p),\ell) &= 1 + S(p,\ell) \\
&\quad \text{if } \ell \in \{boutA(a,b), outA(a,b)\} \\
S(new([c]p)],\ell) &= 1 + S(p,\ell) \\
&\quad \text{if } \ell \in \{boutA(a,b), outA(a,b)\} \\
&\quad \text{and } c \notin \{a,b\} \\
S(new([b]p), boutA(a,b)) &= 1 + S(p, outA(a,b)) \\
S(p,\ell) &= \bot \quad \text{o.w.}
\end{aligned}
$$

Example (Partial Strict Stratification for the π-Calculus)

$$S(out(a,b,p), outA(a,b)) = 0$$
$$S(new([b](out(a,b,p))), boutA(a,b)) = 1$$

$$\dfrac{\dfrac{}{NT[\![out(a,b,p)]\!] \longrightarrow NT[\![(outA(a,b),p)]\!]}\ (\text{Out})}{NT[\![new([b](out(a,b,p)))]\!] \longrightarrow NT[\![(boutA(a,b),p)]\!]}\ (\text{Open})$$

Example (Partial Strict Stratification for the π-Calculus)

$$S(out(a,b,p), outA(a,b)) = 0$$
$$S(new([b](out(a,b,p))), boutA(a,b)) = 1$$

$$\dfrac{\dfrac{}{NT[\![out(a,b,p)]\!] \longrightarrow NT[\![(outA(a,b),p)]\!]}\,(\text{Out})}{NT[\![new([b](out(a,b,p)))]\!] \longrightarrow NT[\![(boutA(a,b),p)]\!]}\,(\text{Open})$$

Example (Partial Strict Stratification for the π-Calculus)

$$S(out(a,b,p), outA(a,b)) = 0$$
$$S(new([b](out(a,b,p))), boutA(a,b)) = 1$$

$$\dfrac{\dfrac{}{NT[\![out(a,b,p)]\!] \longrightarrow NT[\![(outA(a,b),p)]\!]}\ (\text{Out})}{NT[\![new([b](out(a,b,p)))]\!] \longrightarrow NT[\![(boutA(a,b),p)]\!]}\ (\text{Open})$$

Example (Partial Strict Stratification for the π-Calculus)

$$S(out(a,b,p), outA(a,b)) = 0$$
$$S(new([b](out(a,b,p))), boutA(a,b)) = 1$$

$$\dfrac{\dfrac{}{NT[\![out(a,b,p)]\!] \longrightarrow NT[\![(outA(a,b),p)]\!]}\ (\text{Out})}{NT[\![new([b](out(a,b,p)))]\!] \longrightarrow NT[\![(boutA(a,b),p)]\!]}\ (\text{Open})$$

$$S(new([a](in(b,[c]p))), inA(b,c)) = \bot$$

Definition (Alpha-conv.-of-residuals format (ACR format))

Let $\mathcal{R}$ be an NRTSS over Σ_{NTS}, let bn be a binding-names function and let S be a partial strict stratification of $\mathcal{R}$ with respect to bn. Let

$$\frac{\{u_i \longrightarrow (\ell_i, u_i') \mid i \in I\} \qquad \nabla}{t \longrightarrow (\ell, t')}\ \mathsf{Ru}$$

be a rule in $\mathcal{R}$. Let D be the set of variables that occur in the source t of Ru but do not occur anywhere else in the rule.
Ru is in *ACR format with respect to* S iff for each ground substitution φ such that $S(\varphi(t), \ell) \neq \bot$, there exists a ground substitution γ such that $\mathrm{dom}(\gamma) \subseteq D$, and for every atom a in $\mathbb{A} \setminus \{c \in \mathrm{supp}(t) \mid \langle\{c \not\approx t\}\rangle_{nf} = \emptyset\}$ and for every atom $b \in \mathrm{bn}(\ell)$, the following hold:

(i) $\{a \not\approx t'\} \cup \nabla \vdash \{a \not\approx u_i' \mid i \in I\}$,

(ii) $\{a \not\approx t'\} \cup \nabla \cup \{a \not\approx u_i \mid i \in I\} \vdash \{a \not\approx \gamma(t)\}$, and

(iii) $\nabla \cup \{b \not\approx u_i \mid i \in I \wedge b \in \mathrm{bn}(\ell_i)\} \vdash \{b \not\approx \gamma(t)\}$.

$\mathcal{R}$ is in *ACR format with respect to* bn iff $\mathcal{R}$ is in equivariant format and there exists a partial strict stratification S of $\mathcal{R}$ with respect to bn such that all the rules in $\mathcal{R}$ are in ACR format with respect to S.

Alpha-conversion-of-residuals format (ACR format)

Sketch of definition: Given a transition $p \longrightarrow (\ell, q)$ that unifies with the conclusion of a rule, the format ensures that any atom a fresh in (ℓ, q) is also fresh in p, and that any binding atom $b \in \mathrm{bn}(\ell)$ is fresh in p.

Alpha-conversion-of-residuals format (ACR format)

Sketch of definition: Given a transition $p \longrightarrow (\ell, q)$ that unifies with the conclusion of a rule, the format ensures that any atom a fresh in (ℓ, q) is also fresh in p, and that any binding atom $b \in \mathrm{bn}(\ell)$ is fresh in p.

To this end, for each rule

$$\frac{\{u_i \longrightarrow (\ell_i, u_i') \mid i \in I\} \qquad \nabla}{t \longrightarrow (\ell, t')}\ \mathsf{Ru}$$

such that $S(t, \ell) \neq \bot$ the rule format checks the following constraints:

(i) $\{a \not\approx t'\} \cup \nabla \vdash \{a \not\approx u_i' \mid i \in I\}$,

(ii) $\{a \not\approx t'\} \cup \nabla \cup \{a \not\approx u_i \mid i \in I\} \vdash \{a \not\approx t\}$, and

(iii) $\nabla \cup \{b \not\approx u_i \mid i \in I \wedge b \in \mathrm{bn}(\ell_i)\} \vdash \{b \not\approx t\}$.

Alpha-conversion-of-residuals format (ACR format)

Sketch of definition: Given a transition $p \longrightarrow (\ell, q)$ that unifies with the conclusion of a rule, the format ensures that any atom a fresh in (ℓ, q) is also fresh in p, and that any binding atom $b \in \mathrm{bn}(\ell)$ is fresh in p.

To this end, for each rule

$$\frac{\{u_i \longrightarrow (\ell_i, u_i') \mid i \in I\} \qquad \nabla}{t \longrightarrow (\ell, t')}\ \mathsf{Ru}$$

such that $S(t, \ell) \neq \bot$ the rule format checks the following constraints:

(i) $\{a \not\approx t'\} \cup \nabla \vdash \{a \not\approx u_i' \mid i \in I\}$,

(ii) $\{a \not\approx t'\} \cup \nabla \cup \{a \not\approx u_i \mid i \in I\} \vdash \{a \not\approx t\}$, and

(iii) $\nabla \cup \{b \not\approx u_i \mid i \in I \wedge b \in \mathrm{bn}(\ell_i)\} \vdash \{b \not\approx t\}$.

We have obtained these constraints by considering the variable flow in each node of a proof tree and the freshness relations that we want to ensure. The constraints **must be strengthened** by neutralising variables that occur in the source of the rule but nowhere else in the rule, and they **can be relaxed** by ignoring some atoms that for sure are fresh in p.

Alpha-conversion-of-residuals format (ACR format)

Theorem (Rule format for ACR)

Let $\mathcal{R}$ be an NRTSS over Σ_{NTS} and bn be a binding-names function. If $\mathcal{R}$ is in ACR format with respect to bn, then the NRTS induced by $\mathcal{R}$ together with bn constitute an NTS.

That is, the transition relation induced by $\mathcal{R}$ is equivariant and satisfies alpha-conversion of residuals.

Alpha-conversion-of-residuals format (ACR format)

Theorem (Rule format for ACR)

Let $\mathcal{R}$ be an NRTSS over Σ_{NTS} and bn be a binding-names function. If $\mathcal{R}$ is in ACR format with respect to bn, then the NRTS induced by $\mathcal{R}$ together with bn constitute an NTS.

That is, the transition relation induced by $\mathcal{R}$ is equivariant and satisfies alpha-conversion of residuals.

The example NRTSS of the π-calculus is in ACR format, and thus the associated NRTS together with function bn constitute an NTS of [Parrow et al., 2015].