Full Abstraction for Nominal General References

Nikos Tzevelekos
nikt@comlab.ox.ac.uk

LICS, Wroclaw, July 2007

Full Abstraction for Nominal General References – Overview

This talk is about formulating a fully-abstract semantics of nominal general references using nominal games.

We will be talking about:

- Nominal Sets (Gabbay, Pitts)
- A functional higher-order language with nominal general references (Pitts, Stark, NT), the $\nu\rho$-calculus:
  - *good variables (references),*
  - *reference-equality tests.*
- Nominal Games (Abramsky, Ghica, Murawski, Ong, Stark, NT)

Nominal Sets

Assume a countable set of types TY and for each $A \in \mathsf{TY}$ a countably infinite set of *names* N_A. Take,

- $\mathsf{N} \triangleq \biguplus_{A\in\mathsf{TY}} \mathsf{N}_A$ to be the set of *general names*,
- and $\mathsf{PERM}(\mathsf{N}) = \bigoplus_{A\in\mathsf{TY}} \mathsf{PERM}(\mathsf{N}_A)$.

A *nominal set* X is a set equipped with an action from $\mathsf{PERM}(\mathsf{N})$,

$$\_ \circ \_ : \mathsf{PERM}(\mathsf{N}) \times X \to X \qquad (e.g.\ \pi \circ x)$$

such that all $x \in X$ have *finite strong support* $\mathtt{S}(x) \subseteq \mathsf{N}$,

$$\forall \pi \in \mathsf{PERM}(\mathsf{N}).\ \pi \circ x = x \iff \forall \alpha \in \mathtt{S}(x).\pi(\alpha) = \alpha$$

$\rightsquigarrow$ $\mathsf{N}^{\#}$, the set of *finite lists of distinct names*, is a nominal set.
(denote names by $\alpha, \beta, etc.$ and lists of names by $\vec{\alpha}, \vec{\beta}, etc.$)
$\rightsquigarrow$ If X, Y nominal sets then $X \times Y$ a nominal set.

The $\nu\rho$-calculus *–use names for general references!*

The $\nu\rho$-calculus is a functional calculus with nominal references.

$$\mathsf{TY} \ni A, B ::= \mathbb{1} \mid \mathbb{N} \mid [A] \mid A \to B \mid A \otimes B$$

$\mathsf{TE} \ni M, N ::=$	$x \mid \lambda x.M \mid M\,N$	λ-term
	$\mid \mathtt{skip}$	return
	$\mid \tilde{n} \mid \mathtt{pred}\,M \mid \mathtt{succ}\,N$	arithmetic
	$\mid \mathtt{if0}\ M\ \mathtt{then}\ N_1\ \mathtt{else}\ N_2$	if_then_else
	$\mid \langle M, N\rangle \mid \mathtt{fst}\,M \mid \mathtt{snd}\,N$	pair / projections
	$\mid \alpha$	name, $\alpha \in \mathsf{N} = \biguplus_{A\in\mathsf{TY}} \mathsf{N}_A$
	$\mid \nu\alpha.M$	ν-abstraction
	$\mid [M = N]$	name-equality test
	$\mid M := N \mid !M$	update / dereferencing

$$\mathsf{VA} \ni V, W ::= \tilde{n} \mid \mathtt{skip} \mid \alpha \mid x \mid \lambda x.M \mid \langle V, W\rangle$$

The $\nu\rho$-calculus: Typed Terms

Terms are typed in environments $(\vec{\alpha}, \Gamma)$ consisting of:

- *a list* $\vec{\alpha}$ of distinct names ($\vec{\alpha} \in \mathsf{N}^{\#}$)
- a set Γ of variable-type pairs

$\vec{\alpha} \mid \Gamma \vdash M : A$
$\rightsquigarrow$ free vars in Γ
$\rightsquigarrow$ (free) names in $\vec{\alpha}$

$$\frac{}{\vec{\alpha} \mid \Gamma, x:A \vdash x : A} \qquad \frac{}{\vec{\alpha} \mid \Gamma \vdash \alpha : [A]}\ {\scriptstyle \alpha \in \mathsf{S}(\vec{\alpha}) \wedge \alpha \in \mathsf{N}_A}$$

$$\frac{\vec{\alpha}\alpha \mid \Gamma \vdash M : B}{\vec{\alpha} \mid \Gamma \vdash \nu\alpha.M : B} \qquad \frac{\vec{\alpha} \mid \Gamma \vdash M : [A] \qquad \vec{\alpha} \mid \Gamma \vdash N : [A]}{\vec{\alpha} \mid \Gamma \vdash [M = N] : \mathbb{N}}$$

$$\frac{\vec{\alpha} \mid \Gamma \vdash M : [A]}{\vec{\alpha} \mid \Gamma \vdash !M : A} \qquad \frac{\vec{\alpha} \mid \Gamma \vdash M : [A] \qquad \vec{\alpha} \mid \Gamma \vdash N : A}{\vec{\alpha} \mid \Gamma \vdash M := N : \mathbb{1}}$$

The $\nu\rho$-calculus: Reduction

The reduction calculus is defined in store environments S:

$$S ::= \epsilon \mid \alpha, S \mid \alpha :: V, S$$

with their domains being lists of distinct names.

$$\text{EQ}\ \frac{}{S \vDash [\alpha = \beta] \longrightarrow S \vDash \tilde{n}}\ {\scriptstyle n=1 \text{ if } \alpha \neq \beta \\ n=0 \text{ if } \alpha = \beta}$$

$$\text{NEW}\ \frac{}{S \vDash \nu\alpha.M \longrightarrow S, \beta \vDash (\alpha\ \beta) \circ M}\ {\scriptstyle \beta \notin \mathsf{S}(S)}$$

$$\text{DRF}\ \frac{}{S, \alpha :: V, S' \vDash !\alpha \longrightarrow S, \alpha :: V, S' \vDash V}$$

$$\text{UPD}\ \frac{}{S, \alpha(:: W), S' \vDash \alpha := V \longrightarrow S, \alpha :: V, S' \vDash \texttt{skip}}$$

$$\text{LAM}\ \frac{}{S \vDash (\lambda x.M)\, V \longrightarrow S \vDash M\{V/x\}}$$

$\nu\rho$-calculus : Observational Equivalence

Reduction yields the following notion of equivalence.

For typed terms $\vec{\alpha} \mid \Gamma \vdash M : A$ and $\vec{\alpha} \mid \Gamma \vdash N : A$,

$$\vec{\alpha} \mid \Gamma \vdash M \lessapprox N \iff$$
$$\forall \mathrm{C}[\_] : \mathbb{N}.\, (\exists S'.\ \vDash \mathrm{C}[M] \longrightarrow\!\!\!\!\rightarrow S' \vDash \tilde{0}) \implies (\exists S''.\ \vDash \mathrm{C}[N] \longrightarrow\!\!\!\!\rightarrow S'' \vDash \tilde{0})$$

where $\mathrm{C}[\_]$ is a variable- and name-closing context.

For example,

$$\nu\alpha.M \approx M \qquad \text{if } \alpha \notin \mathsf{S}(M)$$
$$\nu\alpha, \beta.M \approx \nu\beta, \alpha.M$$

Game Semantics

Game semantics gained prominence in the mid-90's by providing the first fully abstract semantics for PCF. Since then, game semantics have been used in order to model fully-abstractly languages with a wide range of computational effects –mostly in LICS.

Nominal Games: Arenas and Prearenas

A (nominal) game can be described by *plays* –sequences of moves played in alternation by *Opponent* and *Player*– on a *prearena*.

An *arena* $A \triangleq (M_A, I_A, \vdash_A, \lambda_A)$ is given by:

- A nominal set M_A of moves,
- A nominal subset $I_A \subseteq M_A$ of *initial* moves,
- A nominal *justification* relation $\vdash_A \subseteq M_A \times (M_A \setminus I_A)$,
- A nominal *labeling* function $\lambda_A : M_A \to \{O, P\} \times \{A, Q\}$.

↬ For each $m \in (M_A \setminus I_A)$: $\quad i_A \vdash_A m_1 \vdash_A \cdots \vdash_A m_i \vdash_A m$

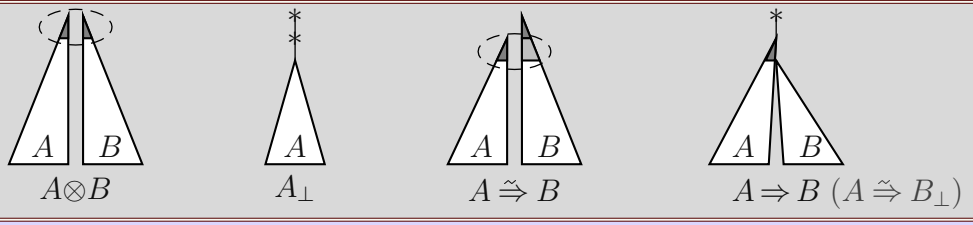
↬ Initial moves are P-Answers,and whenever $m_1 \vdash_A m_2$,

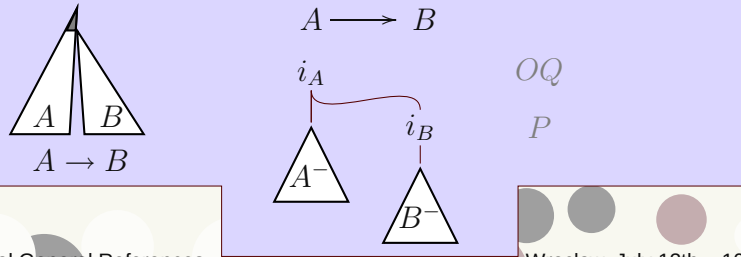
m_1, m_2 by different players , m_1 Answer $\implies$ m_2 Question

A prearena is an arena with its initial moves being O-Questions

Basic Arenas, Prearenas

$$\frac{1}{M_1 \triangleq \{*\} \quad I_1 \triangleq \{*\}} \qquad \frac{\mathbb{N}}{M_{\mathbb{N}} \triangleq \mathbb{N} \quad I_{\mathbb{N}} \triangleq \mathbb{N}} \qquad \frac{N_A}{M_{N_A} \triangleq \mathsf{N}_A \quad I_{N_A} \triangleq \mathsf{N}_A} \qquad \frac{\mathbb{N} \Rightarrow N_A}{* \;\; n \;\; \alpha} \qquad \begin{matrix} PA \\ OQ \\ PA \end{matrix}$$





Moves and Plays

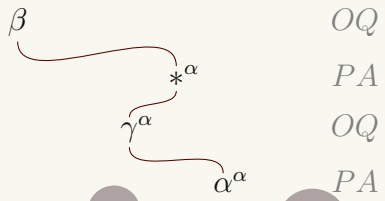
A *move-with-names* of a prearena A is: $m\vec{\alpha}$ ($\vec{\alpha} \in \mathsf{N}^{\#}$ –*local state*, $m \in M_A$)

An $\vec{\alpha}$*-play* on A is a sequence of moves-with-names such that:

- moves are OP-alternating,
- every move is justified by a previous one,
- except from the first move, which is initial and has local state $\vec{\alpha}$,
- Visibility and Well-Bracketing are satisfied.

- O-moves cannot change the local state,
- P-moves can add fresh names to the local state,
- P-moves must add fresh names to the local state to use them,

e.g. $\quad N_A \longrightarrow N_A \Rightarrow N_A$



Strategies

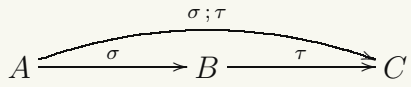
An $\vec{\alpha}$-strategy σ is a prefix-closed and O-move-closed set of equivalence classes $[s]_{\vec{\alpha}}$ of $\vec{\alpha}$-plays, satisfying:

- If even-length $[s_1 x_1]_{\vec{\alpha}}, [s_2 x_2]_{\vec{\alpha}} \in \sigma$ and $[s_1]_{\vec{\alpha}} = [s_2]_{\vec{\alpha}}$ then $[s_1 x_1]_{\vec{\alpha}} = [s_2 x_2]_{\vec{\alpha}}$. *(determinacy)*
- *Innocence* and Totality.

$$[s]_{\vec{\alpha}} \triangleq \{\pi \circ s \mid \pi \circ \vec{\alpha} = \vec{\alpha}\}$$

An $\vec{\alpha}$-strategy σ on $A \to B$ is written $\sigma : A \to B$.

$\sigma : A \to B$ an $\vec{\alpha}$-strategy
$\tau : B \to C$ an $\vec{\alpha}$-strategy



$\sigma ; \tau : A \to C$ an $\vec{\alpha}$-strategy, obtained by:

↝ *composing and hiding B-moves*

↝ *respecting Name Conditions*

Semantics in $\mathcal{V}^{\vec{\alpha}}$

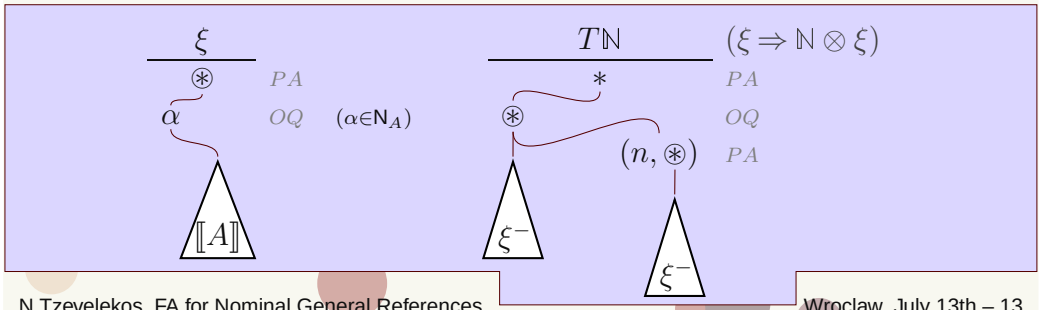
Let $\mathcal{V}^{\vec{\alpha}}$ be the category of nominal arenas and $\vec{\alpha}$-strategies

Translate types to arenas; *solve the following domain equation.*

$$[\![\mathbb{1}]\!] = 1 \qquad [\![\mathbb{N}]\!] = \mathbb{N} \qquad [\![[A]]\!] = N_A \qquad [\![A \otimes B]\!] = [\![A]\!] \otimes [\![B]\!]$$

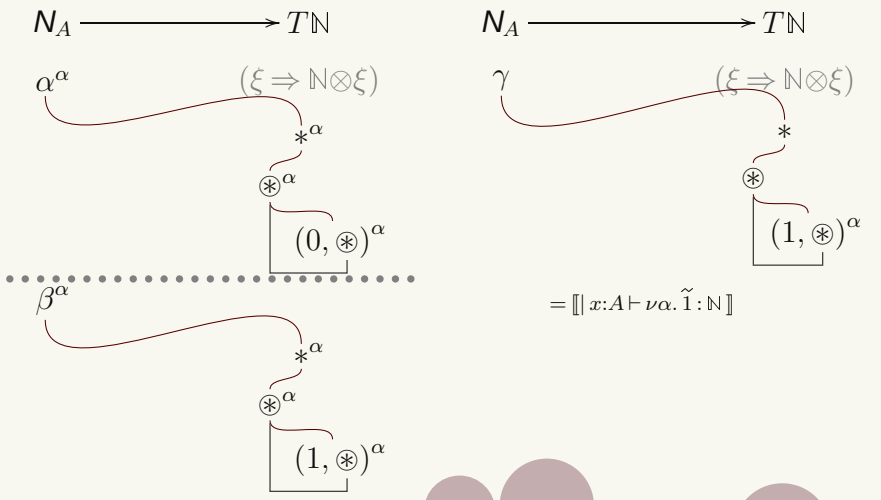
$$[\![A \to B]\!] = [\![A]\!] \otimes \xi \Rightarrow [\![B]\!] \otimes \xi \qquad \xi = \bigotimes_A (N_A \Rightarrow [\![A]\!])$$

We obtain a *store monad* T, taking $TA \triangleq \xi \Rightarrow (A \otimes \xi)$.



Examples of semantics in the model $\mathcal{V} \triangleq \langle \mathcal{V}^{\vec{\alpha}}, T^{\vec{\alpha}} \rangle_{\vec{\alpha} \in \mathsf{N}^{\#}}$

$[\![\, \alpha \,|\, x : A \vdash [x = \alpha] : \mathbb{N} \,]\!]$ $\qquad$ $[\![\, | \, x : A \vdash \nu\alpha.[x = \alpha] : \mathbb{N} \,]\!]$

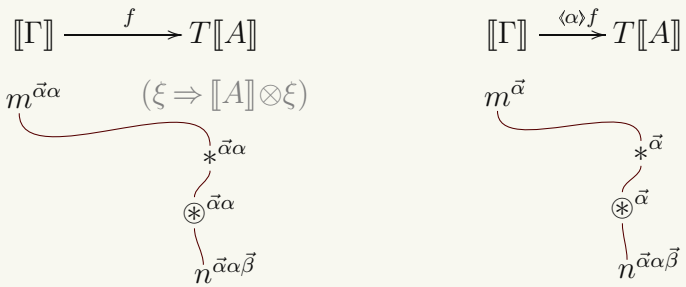


$= [\![\, x{:}A \vdash \nu\alpha.\, \widetilde{1} : \mathbb{N} \,]\!]$

$\mathcal{V}$ is a model of $\nu\rho$

$\rightsquigarrow$ Name-abstraction:

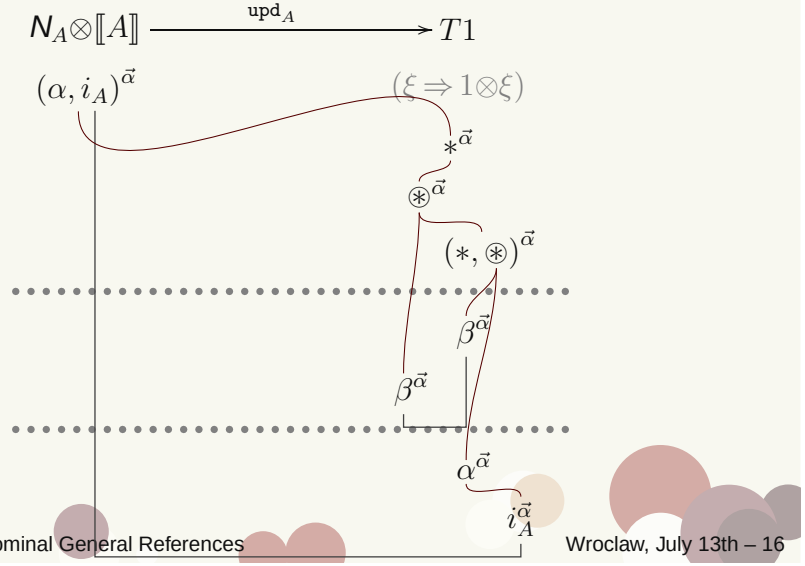
$$\frac{\vec{\alpha}\alpha \mid \Gamma \vdash M : B}{\vec{\alpha} \mid \Gamma \vdash \nu\alpha.M : B} \quad \mapsto \quad \frac{[\![M]\!] : [\![\Gamma]\!] \to T[\![A]\!]}{[\![\nu\alpha.M]\!] = \langle\alpha\rangle [\![M]\!] : [\![\Gamma]\!] \to T[\![A]\!]}$$



$\mathcal{V}$ is a model of $\nu\rho$ (2)

$\rightsquigarrow$ Update: $\quad [\![M]\!] : \Gamma \to TN_A \qquad [\![N]\!] : \Gamma \to TA$

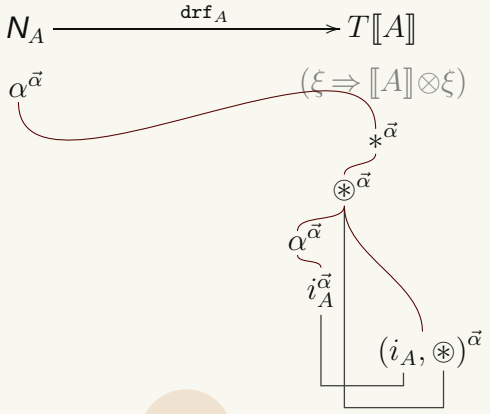
$$[\![M := N]\!] : \Gamma \xrightarrow{\langle [\![M]\!], [\![N]\!] \rangle} TN_A \otimes TA \xrightarrow{\psi} T(N_A \otimes A) \xrightarrow{T\mathtt{upd}_A} T^2 1 \xrightarrow{\mu} T1$$



$\mathcal{V}$ is a model of $\nu\rho$ (3)

$\rightsquigarrow$ Dereferencing:

$$\frac{[\![M]\!] : [\![\Gamma]\!] \to TN_A}{[\![!M]\!] : [\![\Gamma]\!] \xrightarrow{[\![M]\!]} TN_A \xrightarrow{T\mathtt{drf}_A} T^2[\![A]\!] \xrightarrow{\mu} T[\![A]\!]}$$



$\mathcal{V}$ is a sound model

We can show *equational soundness*.

$$[\![M]\!] = [\![N]\!] \implies M \lessapprox N$$

– Do we also have definability? No.

In the reduction calculus the treatment of the store follows a specific *store-discipline*; for example,

- If a store S is updated to S' then the original store S is not accessible any more.
  In strategies stores are treated as variables.
- When the store is asked a name, it either returns its value or it deadlocks; there is no third option.
  When Opponent asks the value of some name, Player is free to evade answering and play elsewhere.

Tidy strategies and Full Abstraction

We therefore restrict strategies by imposing *tidiness conditions*, obtaining thus *tidy strategies*.

Let $\mathcal{T}^{\vec{\alpha}}$ be the subcategory of $\mathcal{V}^{\vec{\alpha}}$ with objects $[\![A]\!]$ and arrows tidy strategies

$\mathcal{T} \triangleq \langle \mathcal{T}^{\vec{\alpha}}, T^{\vec{\alpha}} \rangle_{\vec{\alpha} \in \mathsf{N}^\#}$ is a sound model

---

If $\sigma : [\![A]\!] \to T[\![B]\!]$ is in $\mathcal{T}^{\vec{\alpha}}$ and has *finite description* then it is definable

---

$$[\![M]\!] \lesssim [\![N]\!] \iff M \lessapprox N$$

Last slide, really

Summary:

- $\leadsto$ we introduced $\nu\rho$,
- $\leadsto$ described Nominal Games,
- $\leadsto$ constructed a store arena, and a sound model $\mathcal{V}$,
- $\leadsto$ restricted to tidy strategies to obtain definability, and hence FA.

Further on:

- Names for exceptions and the exception monad
- Abstract categorical models
- ‘Simpler’ quotiening to obtain the ‘nominal’ equalities
- Effectiveness and decidability