An Introduction to Nominal Sets

Andrew Pitts

UNIVERSITY OF CAMBRIDGE

Computer Science & Technology

EWSCS 2020

Lecture 2

Outline

L1 Structural recursion and induction in the presence of name-binding operations.

L2 Introducing the category of nominal sets.

L3 Nominal algebraic data types and α-structural recursion.

L4 Dependently typed λ-calculus with locally fresh names and name-abstraction.

References:

AMP, *Nominal Sets: Names and Symmetry in Computer Science*, CUP 2013

AMP, *Alpha-Structural Recursion and Induction*, JACM 53(2006)459-506.

AMP, J. Matthiesen and J. Derikx,
A Dependent Type Theory with Abstractable Names, ENTCS 312(2015)19-50.

Dependence & Symmetry

What does it mean for mathematical structures [needed for programming language semantics] to

$$\begin{cases} \text{depend upon some names?} \\ \text{be independent of some names?} \end{cases}$$

- Conventional answer: parameterization (explicit dependence via functions).
  Can lead to 'weakening hell'.

Dependence & Symmetry

What does it mean for mathematical structures [needed for programming language semantics] to

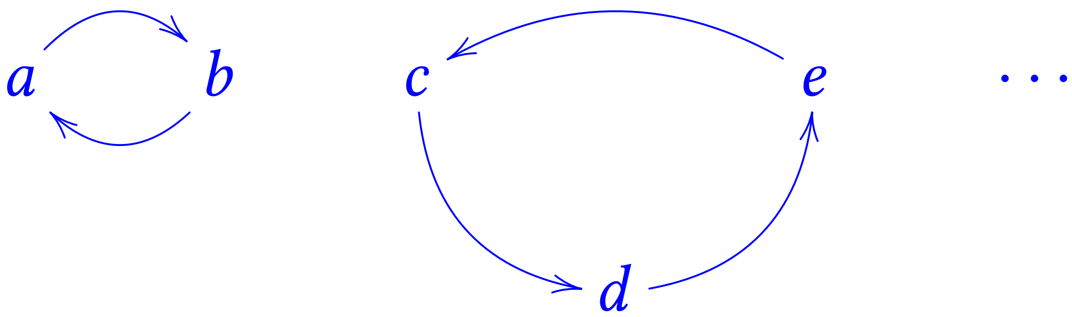
$$\begin{cases} \text{depend upon some names?} \\ \text{be independent of some names?} \end{cases}$$

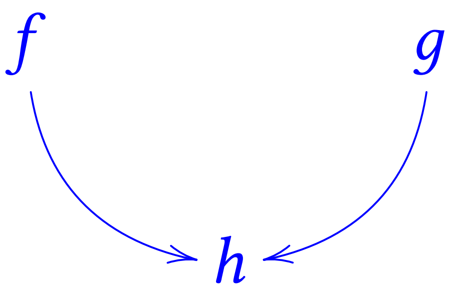
- Conventional answer: parameterization (explicit dependence via functions).
  Can lead to 'weakening hell'.
- *Nominal techniques* answer: independence via invariance properties of symmetries.

Name permutations

- $\mathbb{A}$ = fixed countably infinite set of atomic names (a,b,...)
- Perm $\mathbb{A}$ = group of all (finite) permutations of $\mathbb{A}$

Typical elements:



(but NOT 

)

Name permutations

- $\mathbb{A}$ = fixed countably infinite set of atomic names $(a,b,\ldots)$
- $\mathrm{Perm}\,\mathbb{A}$ = group of all (finite) permutations of $\mathbb{A}$
  - each $\pi \in \mathrm{Perm}\,\mathbb{A}$ is a bijection $\mathbb{A} \cong \mathbb{A}$ (injective and surjective function)
  - π finite means: $\{a \in \mathbb{A} \mid \pi(a) \neq a\}$ is finite.
  - group: multiplication is composition of functions $\pi' \circ \pi$; identity is identity function id; inverses are inverse functions π^{-1}.

Actions

A Perm $\mathbb{A}$-action on a set X is a function

$$\pi \in \mathrm{Perm}\,\mathbb{A},\ x \in X \ \mapsto\ \pi \cdot x \in X$$

satisfying

- $\pi' \cdot (\pi \cdot x) = (\pi' \circ \pi) \cdot x$
- $id \cdot x = x$

Actions

A Perm $\mathbb{A}$-**action** on a set X is a function

$$\pi \in \mathrm{Perm}\,\mathbb{A},\ x \in X \ \mapsto\ \pi \cdot x \in X$$

satisfying

- $\pi' \cdot (\pi \cdot x) = (\pi' \circ \pi) \cdot x$
- $id \cdot x = x$

Simple example: $\mathrm{Perm}\,\mathbb{A}$ acts on sets of names $A \subseteq \mathbb{A}$ via

$$\pi \cdot A = \{\pi(a) \mid a \in A\}$$

E.g.

$$\left(a \;\; b \right) \cdot \{c \mid c \neq a\} = \{c \mid c \neq b\}$$

Running example

Action of $\mathrm{Perm}\,\mathbb{A}$ on set of ASTs for λ-terms

$$Tr \triangleq \{t ::= \mathtt{V}\,a \mid \mathtt{A}(t,t) \mid \mathtt{L}(a,t)\}$$

$$\begin{aligned}
\pi \cdot \mathtt{V}\,a &= \mathtt{V}(\pi\,a) \\
\pi \cdot \mathtt{A}(t,t') &= \mathtt{A}(\pi \cdot t, \pi \cdot t') \\
\pi \cdot \mathtt{L}(a,t) &= \mathtt{L}(\pi\,a, \pi \cdot t)
\end{aligned}$$

This respects α-equivalence [Ex. 1(iii)] and so induces an action on set of λ-terms $\Lambda = \{[t]_\alpha \mid t \in Tr\}$:

$$\pi \cdot [t]_\alpha = [\pi \cdot t]_\alpha$$

Support – the key definition

Suppose $\mathrm{Perm}\,\mathbb{A}$ acts on a set X and $x \in X$.

A set of names $A \subseteq \mathbb{A}$ **supports** x if for all $\pi \in \mathrm{Perm}\,\mathbb{A}$

$$(\forall a \in A.\, \pi(a) = a) \implies \pi \cdot x = x$$

X is a **nominal set** if every $x \in X$ has a finite support. [AMP-Gabbay, LICS 1999]

Fact: one can prove classically (but not constructively) that in a nominal set every $x \in X$ possesses a *smallest* finite support, written $\boxed{\mathrm{supp}\, x}$ (because if finite sets A and B support x, then so does $A \cap B$).

Support – the key definition

Suppose $\mathrm{Perm}\,\mathbb{A}$ acts on a set X and $x \in X$.

A set of names $A \subseteq \mathbb{A}$ **supports** x if for all $\pi \in \mathrm{Perm}\,\mathbb{A}$

$$(\forall a \in A.\, \pi(a) = a) \implies \pi \cdot x = x$$

X is a **nominal set** if every $x \in X$ has a finite support.
[AMP-Gabbay, LICS 1999]

E.g. Tr and Λ are nominal sets—any $\overline{a}$ containing all the variables occurring (free, binding, or bound) in $t \in Tr$ supports t and (hence) $[t]_\alpha$.

Fact: the smallest support for $e \in \Lambda$ is its finite set of *free variables*. [Ex. 2]

Further examples of support

[$\mathrm{Perm}\,\mathbb{A}$ acts on sets of names $S \subseteq \mathbb{A}$ pointwise:
$\pi \cdot S \triangleq \{\pi\, a \mid a \in S\}$.]

What is a support for the following sets of names?

- $S_1 \triangleq \{a\}$
- $S_2 \triangleq \mathbb{A} - \{a\}$
- $S_3 \triangleq \{a_0, a_2, a_4, \ldots\}$, where $\mathbb{A} = \{a_0, a_1, a_2, \ldots\}$

Further examples of support

[$\mathrm{Perm}\,\mathbb{A}$ acts on sets of names $S \subseteq \mathbb{A}$ pointwise:
$\pi \cdot S \triangleq \{\pi\, a \mid a \in S\}$.]

What is a support for the following sets of names?

- $S_1 \triangleq \{a\}$
  Answer: $\{a\}$ is smallest support.
- $S_2 \triangleq \mathbb{A} - \{a\}$
- $S_3 \triangleq \{a_0, a_2, a_4, \ldots\}$, where $\mathbb{A} = \{a_0, a_1, a_2, \ldots\}$

Further examples of support

[$\mathrm{Perm}\,\mathbb{A}$ acts on sets of names $S \subseteq \mathbb{A}$ pointwise:
$\pi \cdot S \triangleq \{\pi\, a \mid a \in S\}$.]

What is a support for the following sets of names?

- $S_1 \triangleq \{a\}$
  Answer: $\{a\}$ is smallest support.
- $S_2 \triangleq \mathbb{A} - \{a\}$
  Answer: $\{a\}$ is smallest support.
- $S_3 \triangleq \{a_0, a_2, a_4, \ldots\}$, where $\mathbb{A} = \{a_0, a_1, a_2, \ldots\}$

Further examples of support

[$\mathrm{Perm}\,\mathbb{A}$ acts on sets of names $S \subseteq \mathbb{A}$ pointwise:
$\pi \cdot S \triangleq \{\pi\, a \mid a \in S\}$.]

What is a support for the following sets of names?

- $S_1 \triangleq \{a\}$
  Answer: $\{a\}$ is smallest support.
- $S_2 \triangleq \mathbb{A} - \{a\}$
  Answer: $\{a\}$ is smallest support.
- $S_3 \triangleq \{a_0, a_2, a_4, \ldots\}$, where $\mathbb{A} = \{a_0, a_1, a_2, \ldots\}$
  Answer: $\{a_0, a_2, a_4, \ldots\}$ is a support

Further examples of support

[$\mathrm{Perm}\,\mathbb{A}$ acts on sets of names $S \subseteq \mathbb{A}$ pointwise:
$\pi \cdot S \triangleq \{\pi\, a \mid a \in S\}$.]

What is a support for the following sets of names?

- $S_1 \triangleq \{a\}$
  Answer: $\{a\}$ is smallest support.
- $S_2 \triangleq \mathbb{A} - \{a\}$
  Answer: $\{a\}$ is smallest support.
- $S_3 \triangleq \{a_0, a_2, a_4, \ldots\}$, where $\mathbb{A} = \{a_0, a_1, a_2, \ldots\}$
  Answer: $\{a_0, a_2, a_4, \ldots\}$ is a support, and so is $\{a_1, a_3, a_5, \ldots\}$—but there is no finite support. S_3 does not exist in the 'world of nominal sets'—in that world $\mathbb{A}$ is infinite, but not enumerable.

Category of nominal sets, **Nom**

objects are nominal sets

= sets equipped with an action of all (finite) permutations of $\mathbb{A}$, all of whose elements have finite support

morphisms are equivariant functions

= functions preserving the permutation action.

$$\pi \cdot (f\,x) = f(\pi \cdot x)$$

identities and **composition**

= as usual for functions

Why use category theory?

- **equivalence of categories** from different mathematical realms (or even just functors between them) can tell us a lot.
  For example, the following are all equivalent:
  - **Nom**
  - the Schanuel topos
    (from Grothendieck's generalized Galois theory)
  - the category of named sets
    (from the work of Montanari *et al* on model-checking π-calculus)
- **universal properties** (adjoint functors) can characterize a mathematical construction uniquely up to isomorphism and help predict its properties.
  For example…

Nominal exponentials

$$\boxed{X \to_{\mathrm{fs}} Y} \triangleq$$

$$\left\{ f \in Y^X \,\middle|\, \begin{array}{l} f \text{ is finitely supported w.r.t. the action} \\ \pi \cdot f = \lambda x \to \pi \cdot (f(\pi^{-1} \cdot x)) \end{array} \right\}$$

This is characterised uniquely up to isomorphism by the fact that it give the right adoint to $(\_) \times X : \mathbf{Nom} \to \mathbf{Nom}$:

$$\frac{Z \times X \to Y}{Z \to (X \to_{\mathrm{fs}} Y)}$$

(Products in $\mathbf{Nom}$ are created by the forgetful functor to the category of sets.)

Nominal exponentials

$X \to_{\mathrm{fs}} Y \triangleq$

N.B. permutations have inverses

$$\left\{ f \in Y^X \;\middle|\; \begin{array}{l} f \text{ is finitely supported w.r.t. the action} \\ \pi \cdot f = \lambda x \to \pi \cdot (f(\pi^{-1} \cdot x)) \end{array} \right\}$$

This is characterised uniquely up to isomorphism by the fact that it give the right adoint to $(\_) \times X : \mathbf{Nom} \to \mathbf{Nom}$:

$$\frac{Z \times X \to Y}{Z \to (X \to_{\mathrm{fs}} Y)}$$

(Products in **Nom** are created by the forgetful functor to the category of sets.)

Category of nominal sets, **Nom**

Nom is a model of classical higher-order logic.

Finite products: $X_1 \times \cdots \times X_n$ is cartesian product of sets with $\mathrm{Perm}\,\mathbb{A}$-action

$$\pi \cdot (x_1, \ldots, x_n) \triangleq (\pi \cdot x_1, \ldots, \pi \cdot x_n)$$

(so $(x_1, \ldots, x_n)$ is supported by $A_1 \cup \cdots \cup A_n$ if each x_i is supported by A_i)

Category of nominal sets, **Nom**

Nom is a model of classical higher-order logic.

Coproducts are given by disjoint union.

Natural number object: $\mathbb{N} = \{0, 1, 2, \ldots\}$ with trivial $\mathrm{Perm}\,\mathbb{A}$-action: $\pi \cdot n \triangleq n$ (so each $n \in \mathbb{N}$ has empty support).

Category of nominal sets, **Nom**

Nom is a model of classical higher-order logic.

Exponentials: $X \rightarrow_{\mathrm{fs}} Y$ …as described previously.

Category of nominal sets, **Nom**

Nom is a model of classical higher-order logic.

Subobject classifier: $\Omega = \{\mathrm{true}, \mathrm{false}\}$ with trivial Perm $\mathbb{A}$-action: $\pi \cdot b \triangleq b$ (so true and false each have empty support).

(**Nom** is a Boolean topos: $\Omega = 1 + 1$.)

Power objects: $\mathrm{P_{fs}}\, X$ = set of subsets $S \subseteq X$ that are finitely supported w.r.t. the Perm $\mathbb{A}$-action

$$\pi \cdot S \triangleq \{\pi \cdot x \mid x \in S\}$$

The nominal set of names

$\mathbb{A}$ is a nominal set once equipped with the action

$$\pi \cdot a = \pi(a)$$

so that each $a \in \mathbb{A}$ is supported by $\{a\}$.

N.B. $\mathbb{A}$ is not $\mathbb{N}$! Although $\mathbb{A} \in \mathbf{Set}$ is a countable, any $f \in \mathbb{N} \to_{\mathrm{fs}} \mathbb{A}$ has to satisfy

$$\{f\,n\} = \mathrm{supp}(f\,n) \subseteq \mathrm{supp}\,f \cup \mathrm{supp}\,n = \mathrm{supp}\,f$$

for all $n \in \mathbb{N}$, and so f cannot be surjective.

Nom $\not\models$ choice

Nom models classical higher-order logic, but <u>not</u> Hilbert's ε-operation $\varepsilon x.\, \varphi(x)$, which satisfies

$$(\forall x : X)\ \varphi(x) \Rightarrow \varphi(\varepsilon x.\, \varphi(x))$$

Theorem. There is no equivariant function $c : \{S \in \mathrm{P_{fs}}\, \mathbb{A} \mid S \neq \emptyset\} \longrightarrow \mathbb{A}$ satsifying $c(S) \in S$ for all non-empty $S \in \mathrm{P_{fs}}\, \mathbb{A}$.

Proof. Suppose there were such a c. Putting $a \triangleq c\, \mathbb{A}$ and picking some $b \in \mathbb{A} - \{a\}$, we get a contradiction to $a \neq b$:

$$a = c\, \mathbb{A} = c((a\ b) \cdot \mathbb{A}) = (a\ b) \cdot c\, \mathbb{A} = (a\ b) \cdot a = b$$

Nom $\not\models$ choice

Nom models classical higher-order logic, but <u>not</u> Hilbert's ε-operation $\varepsilon x.\, \varphi(x)$, which satisfies

$$(\forall x : X)\ \varphi(x) \Rightarrow \varphi(\varepsilon x.\, \varphi(x))$$

In fact **Nom** does not model even very weak forms of choice, such as Dependent Choice.