Nominal duality theory for new, forall, and lambda

Murdoch J. Gabbay

October 15, 2013

Thanks to the organisers for inviting me and organising this event.

Thanks as always to Andrew Pitts—and to Alexander Kurz and Ugo Montanari for inspiration.

A story

I want to tell you a story.

It's about the foundations of computer science.

It's based on nominal techniques and is annotated by papers published over the last twelve years.

Equivariance

First is "Foundations of Nominal Techniques" (BSL, 2011).

This covers analogous material to Andrew's Nominal Sets book (cf. earlier advertisment!).

There is a different emphasis.

Notable is the central position given to the sets cumulative hierarchy and especially to the principle of equivariance:

> *If* $\Phi(x_1, \ldots, x_n)$ *is a predicate in the language of ZFA and* π *is an atoms-permutation then*
> $\Phi(x_1, \ldots, x_n) \Leftrightarrow \Phi(\pi \cdot x_1, \ldots, \pi \cdot x_n)$. *[fountl, Thrm 4.4]*

Often misunderstood, this principle turns long proofs by calculation into one-liners. Very useful in practice.

Equivariance

An informal corollary of equivariance is that a set of atoms is fixed at the start of our reasoning.

Let me ask:

Q. What are atoms used for most?
A. Variable symbols.
Q. What are variable symbols?
A. Syntax for variables.
Q. What are variables?
A. Atoms with a substitution ($s[a:=t]$ or $s[a:=b]$; variables vary).
Q. What is substitution?
A. aha!

What is substitution (take 1)?

One answer: "A study of substitution" (TCS 2009).

The idea:

1. Take an FM set X,
2. split it up into maximal orbits which I can planes—this can be done uniquely—and
3. define substitution in a capture-avoiding manner plane-wise, imitating the capture-avoidance of atoms-abstractions.

Non-trivial because substitution may affect the support of a representative.

This begs generalisation; I haven't got round to doing it.

An FM atom is automagically also a variable ranging over all FM sets!

What is substitution (take 1)?

However: I could get this to commute either with $\cap$ or with $\cup$—but never both. I could also make it commute with Δ (symmetric difference; commutes with $\neg$, like И).

Nice, but useless for modelling the substitution of e.g. fist-order logic, which commutes with $\wedge$ and $\vee$ and $\neg$.

An FM atom may be a variable, but this is for a logic with $\wedge$ or $\vee$, or a logic with Δ, but not a logic with $\wedge$ and $\neg$.

Not a FOL variable (though might be variable of other languages).

Let's try again.

Q. What is substitution (take 2)?

Nominal Algebra (natural extension of nominal rewriting).
Axiomatise substitution as follows:

$$
\begin{array}{lll}
(\sigma\mathbf{a}) & & a[a{\mapsto}x] = x \\
(\sigma\mathbf{id}) & & x[a{\mapsto}a] = x \\
(\sigma\#) & a\#x \Rightarrow & x[a{\mapsto}u] = x \\
(\sigma\alpha) & b\#x \Rightarrow & x[a{\mapsto}u] = ((b\ a){\cdot}x)[b{\mapsto}u] \\
(\sigma\sigma) & a\#v \Rightarrow & x[a{\mapsto}u][b{\mapsto}v] = x[b{\mapsto}v][a{\mapsto}u[b{\mapsto}v]]
\end{array}
$$

This is "Capture-avoiding substitution as a nominal algebra" (ICTAC 2006, FAC 2008).

A. Substitution is σ-algebra: a nominal algebra $\mathcal{X}$ with a function $\sigma : \mathcal{X} \times \mathbb{A} \times \mathcal{X} \to \mathcal{X}$ validating axioms above.

That works. However, it is abstract; still want concrete models.

What is substitution (take 3)?

Use duality. Represent a σ-algebra as the powerset of an $\mathfrak{o}$-algebra:

$$(\mathfrak{o}\sigma) \quad a\#v \Rightarrow p[v\leftarrow\!\!\shortmid b][u\leftarrow\!\!\shortmid a] = p[u[b\mapsto v]\leftarrow\!\!\shortmid a][v\leftarrow\!\!\shortmid b]$$

$\mathfrak{o}$ is a function $\mathfrak{o} : \mathcal{P} \times \mathbb{A} \times \mathcal{P} \to \mathcal{P}$ satisfying the one axiom above. It can be proved that:

- If $\mathcal{P}$ is an $\mathfrak{o}$-algebra then $pow_\sigma(\mathcal{P}) \subseteq pow(\mathcal{P})$ is a σ-algebra.
- If $\mathcal{X}$ is a σ-algebra then $pow_\mathfrak{o}(\mathcal{X}) \subseteq powerset(\mathcal{X})$ is an $\mathfrak{o}$-algebra.

(*powerset* = powerset; *pow* = nominal powerset.)

These things are dual and by construction, the σ-action commutes with $\cap$ and $\cup$.

Astonishing.

What is substitution (take 3)?

Furthermore, the σ-powerset 'creates' universal quantification, and the $\mathfrak{o}$-powerset 'creates' a Leibnitz equality:

$$\begin{aligned} \forall a.X &= \bigcup\{X' \subseteq X \mid a\#X'\} \\ &= \bigcap_u X[a \mapsto u] \\ u =^{\mathcal{P}} v &= \{p \mid И c.p[u \leftarrow\!\shortmid c] = p[v \leftarrow\!\shortmid c]\} \end{aligned}$$

Details are unimportant.

What matters is that duality yields a model of substitution which models first-order logic with equality.

See "Stone-duality for first-order logic" (Howard Barringer Festschrift) and "Semantics out of context" (submitted, arXiv 2013).

What is substitution in the λ-calculus? What is И?

With some modifications—and much work—this apparatus can model substitution, application, and λ in the lambda-calculus, thus giving duality for λ and application ("Representation and duality of the untyped lambda-calculus" arXiv 2013).

With major simplifications (including removal of σ) this apparatus models atoms with a И-quantifier, thus giving duality for И ("Stone duality for nominal Boolean algebras with New" CALCO 2011).

Deep breath

A coherent view of names and variables in foundations is emerging.

The relationship between names and variables is clearer—and there is more to it than inductive syntax!

Axiomatise desired properties, then build concrete nominal/FM sets models. Creativity involved in determining the 'dual structure'.

This works for overtly logical systems such as Boolean algebras with NEW (Banonas) and first-order logic with equality (FOLeq algebras)—and for less evidently logical structures, like the untyped λ-calculus (inDi$\forall_\bullet$s).

It gets even better:

Lattices and limits

Assume a distributive lattice $(\mathcal{X}, \leq, \wedge, \vee)$ in nominal sets. So in particular given $x, y \in \mathcal{X}$ we have a limit

$$x \wedge y, \textit{ greatest lower bound for } \{z \mid z \leq x,\ z \leq y\}.$$

Now $\mathcal{X}$ is a nominal set. So, given $x \in \mathcal{X}$ assume we have

$$\forall a.x \textit{ greatest lower bound for } \{z \mid z \leq x,\ a\#z\}.$$

This is a finite nominal limit (a 'limit-subject-to-freshness').

$\forall a.x$ is the largest element below x for which a is fresh.

For those who think in orbits:

$$\forall a.x \textit{ greatest lower bound for orbit-finite set } z\overset{a}{\circlearrowleft} = \{\pi \cdot x \mid \pi \in \mathit{fix}(\mathrm{supp}(z) \backslash \{a\})\}.$$

Easy proof.

Lattices and limits

So fresh-finite limits = limits of orbit-finite lattice subsets.

Fresh-finite limits admit a nominal algebra axiomatisation—and in presence of σ other characterisations, such as:

- intersections of all substitution instances $\bigcap\{x[a{\mapsto}u] \mid \text{all } u\}$ &
- limits of strictly (uniformly) finitely supported sets $\bigcup\{x' \mid \mathrm{supp}(x') \subseteq \mathrm{supp}(x) \setminus \{a\}\}$.

"Nominal semantics for predicate logic" (CILC 2012), "Semantics out of context" (arXiv 2013).

We can now answer our questions as follows:

- 'Variable' = 'atom in a σ-algebra'.
- This algebra may have further properties, characterised in algebras or lattices (or topologies; elided).
- Concrete representations obtained naturally, if not easily, by Stone or spectral space constructions.
- Specific examples include *И* (*sans* substitution by design), first-order variables with $\forall$ and $=$, and λ-calculus.
  I expect π-calculus is possible, but I haven't done that.

My story is this:

It is possible to found computer science purely in nominal sets and the FM cumulative hierarchy.

You don't need inductive syntax and Tarski-style valuation semantics to give meaning to syntax or semantics of logic and computation.

It can be constructed directly using nominal powersets, just as for Boolean algebras.