Nominal sets and the И-quantifier
Joint work with Daniela Petrişan and Tadeusz Litak

École Polytechnique, France

Murdoch J. Gabbay

October 7, 2010

The title of this talk

I know it differs from that advertised.

The content of the talk has not changed; it was always going to be about "the last thing I've done that I want to tell you about".

I thought I might tell you a little bit about some current work on representing the $\mathit{И}$-quantifier.

I'll tell you what that is in a moment.

Thanks

For me going to LIX is exciting like going to summer camp was as a teenager. I meet people with new ideas that I can think about for months.

Many thanks to DIGITEO, Gilles Dowek, and Assia Mahboubi for making it possible for me to be here today.

On the importance of names

It is almost impossible to construct a logic or programming language that does not include names (referents).

Names necessarily arise for any language or logic for incompleteness, connectedness, information flow, locality, choice, or quantification.

With specific regard to what happens here in LIX and INRIA, think of variable symbols, variables, channel names, nonces, universal/existential variables, and memory addresses.

A semantics for names

Despite these different uses, names seem to make similar contributions to systems that contain them.

I would argue that we are lacking a unified account of the nature of names that accounts for their common features, and explains their indispensability.

A semantics for the behaviour of names is required: be it for logic, computation, or human communication.

Mathematics in ZFA

Zermelo-Fraenkel (ZF) set theory and Higher-Order Logic do not include a semantic category for names. ZF starts from the empty set and builds upwards using powersets. Higher-Order Logic starts from o and builds upwards using function-spaces.

Names are a syntactic category; variable symbols. Their field of possible denotations is a semantic category; denotations (sets/functions). This is useful if it is the behaviour of the denotations we are interested in, but it is less helpful if we wish to study how names themselves behave.

In 2004 I was working at LIX. At the time, (at least) three people were thinking about extending denotations with names: me, Dale Miller, and Gilles Dowek.

It is unfortunate that were were pairwise incomprehensible. Since then, however, we have moved closer together.

On mathematical models and cornflour

Planners of research and devisers of research metrics take note.

It can easily take six years for the consequences of research to begin to manifest themselves.

Mathematical models of research are like cornflour *(farine de maïs)*.

If you just throw it into the pot and stir without understanding what you're doing, then you get a load of thick lumps (*grumeaux/balourds*) and you ruin the sauce.

What are nominal techniques?

OK, so what are nominal techniques?

We build our mathematical universe using atoms $a \in \mathbb{A}$ (set-theorists: urelemente; process calculists: names; category-theorists: Schanuel topos).

For set theorists: we use Zermelo-Fraenkel sets with atoms (we start from atoms $\mathbb{A} = \{a, b, c, \ldots\}$ instead of from $\varnothing$).

Names are data; atoms. $\mathbb{A}$ (the set of atoms) is a datatype of names.

Symmetry properties of atoms—e.g. that atoms are symmetric under permutation—directly import into the nominal metatheory.

Thus, we do not only get a new datatype $\mathbb{A}$; we get a new meta-theory, and thus to new logic and programming principles.

The new meta-theory: equivariance

Because atoms are atomic, we can permute them without affecting truth. Truth is symmetric under permuting atoms:

Principle of Equivariance $\qquad\qquad \phi \Leftrightarrow \pi{\cdot}\phi$

π is a bijection on atoms. i.e. $a = b$ if and only if $b = a$.

The logic/programming principle this corresponds to is α-renaming.

Because this works for the whole universe we get names and binding in semantic objects like functions, graphs, games, and so on.

The new meta-theory: the И-quantifier

Names can be 'generated fresh':

The NEW quantifier $\quad И a.\phi(a) \Leftrightarrow \{a \mid \neg\phi(a)\}$ is finite

$И a.\phi(a)$ means 'ϕ holds of most atoms'. Thus $И a.a \notin fv(t)$. Dale Miller was, and still is, studying the ∇-quantifier. For our purposes now, this is the same thing as И.

This corresponds to locality, capture-avoidance, and dynamic allocation; *gensym*, name-restriction in the π-calculus, freeness side-conditions in proof-search, and so on.

The new meta-theory: freshness and support

Atoms can be 'free in' elements:

Freshness	$a\#x \Leftrightarrow И b.(b\ a)\cdot x = x$
Support	$supp(x) = \{a \mid И b.(b\ a)\cdot x \neq x\}$

This corresponds to independence or separation.

Call x finitely-supported when $supp(x)$ exists (if it exists, it is finite).

This corresponds to free variables of, but again valid for the whole universe. Call a set x nominal when x is finitely-supported and $supp(x)$ exists. (Slight abuse of notation.)

From the general to the specific

This concludes the general principles.

I will now sketch some mathematical specifics of finite support and the $И$-quantifier.

Axiomatic properties of и

It is possible to write down axioms for Boolean logic with и. We use nominal algebra; universal algebra enriched with freshness and permutations (see "Nominal Universal Algebra" with Mathijssen, JLC 2009).

(**Commute**)		$x \wedge y = y \wedge x$
(**Assoc**)		$(x \wedge y) \wedge z = x \wedge (y \wedge z)$
(**Huntington**)		$x = \neg(\neg x \wedge \neg y) \wedge \neg(\neg x \wedge y)$
(**Swap**)		$\text{и}a.\text{и}b.x = \text{и}b.\text{и}a.x$
(**Garbage**)	$a\#x \Rightarrow$	$\text{и}a.x = x$
(**Distrib**)		$\text{и}a.(x \wedge y) = (\text{и}a.x) \wedge (\text{и}a.y)$
(**SelfDual**)		$\neg\text{и}a.x = \text{и}a.\neg x$
(**Alpha**)	$b\#x \Rightarrow$	$\text{и}a.x = \text{и}b.(b\ a)\cdot x$

These are all valid properties of the и-quantifier in ZFA.

The nominal powerset and the sets version n of И

The nominal powerset $pow(\mathsf{X})$ is the set of finitely-supported subsets of X.

Given finitely-supported $X \subseteq \mathsf{X}$ define

$$\mathsf{n}a.X = \{x \mid И b.(b\ a)\cdot x \in X\}.$$

Easy lemma: $Иa.\phi(a)$ holds precisely when $a \in \mathsf{n}a.\{a \mid \phi(a)\}$.

So n reflects И into nominal sets.

If we translate $\wedge$ as $\cap$, $\neg$ as $\setminus$, and И as n, then we get a model of the axioms above.

Stone duality

So we have reflected the nominal meta-theory into powersets, and into algebra.

Question: Are these two reflections correct in the sense that every model of the axioms is a submodel of a nominal powerset; and do we get a Stone duality?

Answer (according to Gabbay, Petrișan, Litak 2010): Yes.

Boolean algebra with $И$ is dual to a notion of Stone space with n.

I will sketch how the representation theorem works.

I will do this only very briefly, considering the critical points where cornflour has to be added in just the right manner so as to make the sauce work.

The usual squiggles

Usually, we proceed as follows: given B we build an underlying set $\mathrm{B}^\bullet$ out of points, which are maximal filters. A filter is a set $X \subseteq \mathrm{B}$ such that:

- $\bot \notin X$.
- $x \in X \wedge y \in X$ if and only if $x \wedge y \in X$.

A filter is maximal when $p \subseteq p'$ implies $p' = p$.

We then map $x \in \mathrm{B}$ to $x^\bullet = \{p \mid x \in p\}$. This turns out to be an injection (we use Zorn's lemma) and a homomorphism of Boolean algebras. So we have injected B into the powerset of points of B.

That's the 'classical' proof. Several things go wrong in the nominal case.

The usual squiggles

Several things go wrong in the nominal case:

- Zorn's lemma is not true in nominal sets.
- The map $\text{-}^\bullet$ does not commute with и. That is, $(\text{и}a.x)^\bullet \neq \text{n}a.(x^\bullet)$. So $\text{-}^\bullet$ would not be a homomorphism even if it existed.
- A technical construction in the proof where be build a filter $z\uparrow = \{x \mid z \leq x\}$, just does not seem to work. I cannot give you a good intuition as to why; the proofs just break. The 'classical' notion of filter is somehow too general.

All of the difficulties can be overcome.

The nominal squiggles

Suppose we have B an abstract nominal Boolean algebra with $\mathit{и}$.

An n-filter is a finitely-supported subset $p \subseteq |\mathrm{B}|$ such that:

1. $\bot \notin p$.
2. $\forall x, y.(x \in p \wedge y \in p) \Leftrightarrow (x \wedge y \in p)$.
3. $\mathit{И}a.\forall x.x \in p \Rightarrow \mathit{и}a.x \in p$.

The last condition is 'magic sauce' to make the proofs go through.
It corresponds to the following observation about nominal sets:
$\mathit{И}a.x \in X \Leftrightarrow x \in \mathrm{n}a.X$.

Lemma: If p is maximal then the reverse implication must hold.

More squiggly bits

Zorn's lemma fails in nominal sets.

To be more precise, Zorn's lemma is consistent with ZFA but the least upper bound of a chain of finitely-supported elements need not be finitely-supported.

Definition: Call $Y \subseteq X$ bounded-supported when $\bigcup\{supp(x) \mid x \in Y\}$ is finite.

Nominal Zorn: Consider $\leq \subseteq X \times X$ a partial order on X such that any totally (linearly) ordered finitely-supported set $C \subseteq X$ has an upper bound $b(C)$ such that $supp(b(C)) \subseteq supp(C)$. Then every nonempty bounded-supported set $Y \subseteq X$ has a maximal element.

One more little bit of magic sauce

The following lemma lets nominal Zorn give us maximal filters:

Lemma: p is a maximal n-filter if and only if it is maximal amongst p' such that $supp(p') \subseteq supp(p)$.

Modulo a few further technical subtleties, the proof now goes through. Given B we build a powerset out of maximal n-filters and inject B into it by mapping x to $\{p \mid x \in p\}$.

Then $\wedge$ maps to $\cap$, $\neg$ maps to $\setminus$, and и maps to n.

It is possible to extend this to a notion of nominal Stone space with n and a duality.

Conclusions

We have touched on the following in this talk:

- Advantages of doing computer science in a universe with atoms.
- Permutation symmetry properties of such a universe, and the consequences in terms of logic and programming.
- The И-quantifier for dynamic allocation/fresh name generation.
- Nominal algebra; a universal algebra for nominal sets.
- Axiomatising И and reflecting it into nominal powersets (the function n).
- Duality of the axioms and the 'topological' treatments.

Future work

Suggestion: sets interpretation and representation theorem for ∇.

Suggestion: similar treatment of other structure of nominal sets, such as:

- $\nu a.X = \{\pi{\cdot}x \mid x \in X,\ \pi \in \mathit{fix}(\mathit{supp}(X)\backslash\{a\})\}$ (this is basically atoms-abstraction $[a]x$ or if you prefer presheaves, it is δ).
- $X_{\#a} = \{x \in X \mid a\#x\}$.

Suggestion: prove that our axioms for И uniquely characterise и on nominal powersets.

Suggestion: mix и with axioms for other connectives and see what kind of sauce we get!

Deeper message

Names are not just symbols in syntax; α-equivalence is not just an inductive relation.

They are part of a broader foundational issue which is on a par with numbers, sets, and functions, and which can be apprehended as a topic in its own right.

The issues thus raised have linguistic, semantic, proof-theoretic, and computational aspects.