Nominal Sets, Equivariance Reasoning, and Variable Binding

Murdoch J. Gabbay mjg1003@cl.cam.ac.uk
Computer Laboratory, Cambridge University, UK

1  Equivariance reasoning

FM techniques are a methodology of thinking about syntax and in particular about syntax with binding. They take their name from the original FM (Fraenkel-Mostowski) theory of sets presented in my thesis [4]. For this document we use a different way of presenting FM techniques based on the idea of a Nominal Set, which is a set equipped with certain algebraic properties (just as a group, ring, or field, is a set equipped with certain properties), see Definition 1.2. First we need background machinery:

Definition 1.1. Fix a countably infinite set of atoms $\mathbb{A}$. Write typical elements $a, b, c, \ldots \in \mathbb{A}$. For $a, b \in \mathbb{A}$ write $(a \circ b)$ for the function $\mathbb{A} \to \mathbb{A}$ such that $a \mapsto b$ and $b \mapsto a$ and $n \mapsto n$ for all other atoms $n \neq a, b$. This is a bijection with inverse itself, write $\mathbb{P}_a$ for the group generated by $(a \circ b)$ for all $a, b \in \mathbb{A}$ under functional composition $\circ$. Write typical elements $\pi, \pi' \in \mathbb{P}_a$ and $I_{d} \in \mathbb{P}_a$ for the identity.

Definition 1.2. A Nominal Set is a pair $(X, \cdot)$ of an underlying set $X$ and permutation action $\cdot$ (written infix) of type $\mathbb{P}_a \times X \to X$ and satisfying the usual axioms, namely $\pi \cdot (\pi' \cdot x) = \pi \circ \pi' \cdot x$ and $I_{d} \cdot x = x$. The permutation action also satisfies a finiteness condition omitted here.\footnote{See [3, eq. 3], [5, eq. 4], and 'finite support' in [2, Def. 3.3].}

The point is that finite labelled trees, and hence the standard model of syntax but also a natural model of proofs as trees, are Nominal Sets: the permutation action is given pointwise by the action on the labels. Thus for example natural numbers $\mathbb{N}$ satisfy a trivial permutation action given by $\pi \cdot n = n$ always. A datatype of trees for terms of the $\lambda$-calculus (using $\mathbb{A}$ as variable names)

$$\Lambda \cong \mathbb{A} + \Lambda \times \Lambda + \Lambda \times \Lambda$$

is also a Nominal Set with the permutation action given pointwise by the action on the atoms labelling the tree. Furthermore we can represent a theory of $\alpha$-equivalence on these terms as a subset of "well-formed" trees in the inductively defined set

$$T \cong \mathbb{A} + T \times T + \Lambda \times T \times T,$$

namely those inductively constructed using the rules

$$a =_{\alpha} a \quad (\text{Var}) \quad \frac{t_1 =_{\alpha} t_1' \quad t_2 =_{\alpha} t_2'}{t_1 t_2 =_{\alpha} t_1' t_2'} \quad (\text{App}) \quad \frac{t\{c/a\} =_{\alpha} t'\{c/a'\}}{\lambda a t =_{\alpha} \lambda a' t'} \quad (\text{Lam})$$

where in (Lam) there is a side-condition that $c \notin \{a, a'\} \cup n(t) \cup n(t')$ (thus 'fresh' for the conclusion). The usefulness of this way of looking at syntax and properties of syntax as Nominal Sets begins with the following trivial theorem:

Theorem 1.3. If a property (on trees) is defined (inductively) using predicates whose validity is invariant under permuting atoms, then the property is invariant under permuting atoms.

Here "invariant under permuting..." means "given some valid instance of the property, a permutation $\pi$ uniformly applied to its arguments yields another valid instance".

We have an example in the property of well-formedness of proof-trees of $=_{\alpha}$ given in (3). $a =_{\alpha} a$ is a valid instance of (Var) and if we apply $(b \ a)$ to this we obtain $b =_{\alpha} b'$ which is also a valid instance of
(Var). The case of (App) is simple. A permutation applied to a valid instance of (Lam) is also a valid instance of (Lam) because $c \notin \{a, a'\} \cup (t \cup t')$ if and only if $\pi \cdot c \notin \{\pi \cdot a, \pi \cdot a'\} \cup (\pi \cdot t \cup (\pi \cdot t'))$.

We now have a very concrete demonstration that proofs of $=_{\alpha}$ are invariant under permutation; we permute the atoms in the proof as a tree. We can take this further. Consider proving transitivity of $=_{\alpha}$ by induction on proof-trees. The induction predicate is (in words) "given a valid proof-tree $\Pi$ concluding in $t =_{\alpha} t'$, for all valid proof-trees $\Pi'$ concluding in $t' =_{\alpha} t''$, there exists a valid proof-tree $\Pi''$ concluding in $t =_{\alpha} t'''$. This property is constructed using predicates invariant under permutations (validity of proofs of $=_{\alpha}$) and so is itself invariant under permutations. Thus from Theorem 1.3 we know if we have the inductive hypothesis of $\Pi$, we have it of $\pi \cdot \Pi$ for any permutation $\Pi$.

We proceed by induction on $\Pi$. The case of (Lam) for $t = \lambda a s$ and $t' = \lambda a's'$ causes problems: we may assume $\Pi$ proves $s[c/a] =_{\alpha} s'[c'/a']$ and $\Pi'$ proves $s'[c'/a'] =_{\alpha} s''[c'/a'']$ and we assume the inductive predicate for $\Pi$, but we do not know $c = c'$ so we cannot proceed. However, we can apply a permutation $(d c)$ to $\Pi$, and $(d c')$ to $\Pi'$, for $d$ chosen completely fresh. Now we have valid proofs $(d c) \cdot \Pi$ concluding in $s[d/a] =_{\alpha} s'[d/a']$ and $(d c') \cdot \Pi'$ concluding in $s'[d/a'] =_{\alpha} s''[d/a'']$, and also the inductive predicate for $(d c) \cdot \Pi$. We can now complete the proof of transitivity.

Just these ideas of permutations have already been adopted and put to use by other authors also in published work (see for example [6]).

2 Taking it further

There is an equivalence class of proofs concluding in $\lambda at =_{\alpha} \lambda a't'$, one for each fresh $c$; we can take it as an object in its own right. This is an instance of FM abstraction $\text{[A]}X$ which exists for any Nominal Set $X$ by virtue of the permutation action, which lets us rename atoms and construct an equivalence class in the general case (see [2, Section 5]). We can apply this to syntax as well as proofs:

$$\Lambda_{\alpha} \cong A + \Lambda_{\alpha} \times \Lambda_{\alpha} + [A]\Lambda_{\alpha}$$

(4)

is a datatype of $\lambda$-terms up to $\alpha$-equivalence. An element of $[A]\Lambda_{\alpha}$ is (concretely) an equivalence class of pairs $(a, t)$ for $a \in A$ a 'bound atom' fresh for the other atoms in the 'body' $t \in \Lambda_{\alpha}$.

There are various ways of taking this further; Nominal Sets form a category, the Schanuel Topos. Because it is a topos we can construct a general theory of abstractions and equivalence reasoning within it (this is FMCat in [5, Section 2], see also [2, p.21]). Nominal Sets are also a special case of a general theory of FM sets, see [4] and [2]. Nominal Sets can be axiomatised in first-order logic, see [7]. A team in Cambridge has developed FreshML, a programming language based on these principles in which we can program using abstractions and permutations, see [1]. Finally, I am currently implementing FM sets in Isabelle, see [4]. Further reading can be found in any of the references below, and my homepage www.cl.cam.ac.uk/~mjg1003.

References


---

2This is not the case if we try to base the theorem on substitutions generated by $[b/a]$ instead of permutations generated by $(b a) = [b/a, a/b]$. 