

# Nominal Equational Logic

Ranald Clouston

From work with Andrew Pitts

ICMS - Mathematical Theories of Abstraction, Substitution and Naming in  
Computer Science

27 May 2007

## Overview

**Equational logic**, the logic for equality within *sets*, is used throughout computer science.

The aim of our work is to lift this well understood logic, with minimal redesigning, to the world of *nominal sets*.

This will allow us to reason about equality judgements that are modulated by freshness judgements;

$$a \# x \implies x = \lambda a.x a \text{ (\eta-conversion)}$$

and about freshness judgements directly:

$$a \# \lambda a.x \text{ (\alpha-conversion)}$$

## Signatures

An NEL-*signature*  $\Sigma$  is specified by

- A set  $\text{Sort}_\Sigma$ , the *sorts* of  $\Sigma$ ;
- A **nominal set**  $\text{Op}_\Sigma$ , the *operation symbols* of  $\Sigma$ ;
- An equivariant function assigning to each  $op \in \text{Op}_\Sigma$  an arity  $\vec{s} \rightarrow s$ , where  $\vec{s}$  is a (possibly empty) list of sorts.

The equivariance of the arity functions means that  $op$  and  $\pi \cdot op$  have the same arity for any permutation  $\pi$ .

We can split  $\text{Op}_\Sigma$  up into nominal subsets  $\text{Op}_\Sigma(\vec{s}, s)$  for each arity  $\vec{s} \rightarrow s$ .

**Example:** Nominal substitution (Fiore & Staton, LICS 2006):

$$\text{Sort}_\Sigma = \{s\}, \text{Op}_\Sigma([s], s) = \{[b/a] \mid (b, a) \in \text{Atom} \times \text{Atom}\}$$

## Structures

A  $\Sigma$ -structure  $M$  is specified by

- A nominal set  $M[[s]]$  for each sort  $s \in \text{Sort}_\Sigma$ ;
- An equivariant function

$$M[[ - ]] : \text{Op}_\Sigma(\vec{s}, s) \rightarrow (M[[\vec{s}]] \rightarrow_{f_s} M[[s]])$$

for each  $s, \vec{s} = [s_1, \dots, s_n]$ , where  $M[[\vec{s}]]$  is the product  $M[[s_1]] \times \dots \times M[[s_n]]$ .

So each  $M[[op]]$  is a finitely supported function. The requirement that  $M[[ - ]]$  be equivariant ensures that  $a \# op \implies a \# M[[op]]$ .

## Terms and Values

Given a countably infinite set  $\text{Var}$  of variables;

$$t ::= \pi x \mid op\ t \cdots t$$

where  $\pi$  is a finite atom-permutation,  $x \in \text{Var}$  and  $op \in \text{Op}_\Sigma$ . Given an assignment of sorts to variables, terms are sorted as one would expect.

We write  $x$  for  $\iota x$ , where  $\iota$  is the identity permutation.

Now suppose we have a *valuation*  $\rho$  mapping each variable  $x$  of sort  $s$  to a member of  $M[[s]]$ . Then the *value*  $M[[t]]\rho$  of term  $t$  is defined by:

$$\begin{aligned} M[[\pi x]]\rho &\triangleq \pi \cdot \rho(x) \\ M[[op\ t_1 \cdots t_n]]\rho &\triangleq M[[op]](M[[t_1]]\rho, \dots, M[[t_n]]\rho) . \end{aligned}$$

## Judgements and Theories

A *freshness environment*  $\nabla$  is a finite list

$$[\bar{a}_1 \# x_1 : s_1, \dots, \bar{a}_n \# x_n : s_n]$$

where each  $\bar{a}_i$  is a finite set of atoms asserted to be fresh for the variable  $x_i$ .

A *judgement* has the form

$$\nabla \vdash \bar{a} \# t \approx t' : s$$

where  $\bar{a}$  is a finite list of atoms and  $t, t'$  have the same sort  $s$ . We write

$$\nabla \vdash t \approx t' : s \text{ for } \nabla \vdash \emptyset \# t \approx t' : s;$$

$$\nabla \vdash \bar{a} \# t : s \text{ for } \nabla \vdash \bar{a} \# t \approx t : s.$$

A *theory*  $\mathbb{T}$  is a collection of judgements.

## Algebras

Given a freshness environment  $\nabla$  and valuation  $\rho$ , we write  $\rho \in M[\nabla]$  if  $(\bar{a} \# x : s) \in \nabla$  implies  $\bar{a} \# \rho(x) \in M[s]$ .

A  $\Sigma$ -structure  $M$  *satisfies* a judgement

$$\nabla \vdash \bar{a} \# t \approx t' : s$$

if for all  $\rho \in M[\nabla]$ ,  $\bar{a} \# M[t]\rho$  and  $M[t]\rho = M[t']\rho$ . A  $\mathbb{T}$ -*algebra* is a structure that satisfies all the axioms of a theory  $\mathbb{T}$ .

We write

$$\nabla \vDash_{\mathbb{T}} \bar{a} \# t \approx t' : s$$

if the judgement is satisfied by all  $\mathbb{T}$ -algebras.

## Example: Nominal Substitution

$\text{Sort}_\Sigma = \{s\}$ ,  $\text{Op}_\Sigma([s], s) = \{[b/a] \mid (b, a) \in \text{Atom} \times \text{Atom}\}$

1.  $x \vdash a \not\# [b/a]x$
2.  $x \vdash [a/a]x \approx x$
3.  $a \not\# x \vdash [b/a]x \approx x$
4.  $x \vdash [b/a][a/b]x \approx [b/a]x$
5.  $x \vdash [c/b][b/a]x \approx [c/b][c/a]x$
6.  $x \vdash [c/b][c/a]x \approx [c/a][c/b]x$
7.  $x \vdash [d/b][c/a]x \approx [c/a][d/b]x$

(Fiore & Staton, LICS 2006)

## Proof Rules I

$$\begin{array}{c}
 \text{(REFL)} \frac{}{\nabla \vdash t \approx t : s} \quad t \text{ HAS SORT } s \qquad \text{(SYMM)} \frac{\nabla \vdash \bar{a} \# t \approx t' : s}{\nabla \vdash \bar{a} \# t' \approx t : s} \\
 \\
 \text{(TRANS)} \frac{\nabla \vdash \bar{a}_1 \# t \approx t' : s \quad \nabla \vdash \bar{a}_2 \# t' \approx t'' : s}{\nabla \vdash (\bar{a}_1 \cup \bar{a}_2) \# t \approx t'' : s} \\
 \\
 \text{(SUBST)} \frac{\nabla' \vdash \sigma \approx \sigma' : \nabla \quad \nabla \vdash \bar{a} \# t \approx t' : s}{\nabla' \vdash \bar{a} \# t\{\sigma\} \approx t'\{\sigma'\} : s} \quad \sigma, \sigma' \in \Sigma(\nabla, (\nabla')) \\
 \\
 \text{(WEAK)} \frac{\nabla \vdash \bar{a} \# t \approx t' : s}{\nabla' \vdash \bar{a} \# t \approx t' : s} \quad \nabla \leq \nabla'
 \end{array}$$

## Proof Rules II

$$\text{(ATM-INTRO)} \frac{\nabla \vdash \bar{a} \# t \approx t' : s}{\nabla^{\#a} \vdash \bar{a} \cup \{a\} \# t \approx t' : s} \quad a \text{ DOES NOT APPEAR IN } (\bar{a}, t, t')$$

$$\text{(ATM-ELIM)} \frac{\nabla^{\#a} \vdash \bar{a} \# t \approx t' : s}{\nabla \vdash \bar{a} \# t \approx t' : s} \quad a \text{ DOES NOT APPEAR IN } (\nabla, \bar{a}, t, t')$$

$$\text{(\#-EQUIVAR)} \frac{}{\bar{a} \# x : s \vdash \pi \cdot \bar{a} \# \pi x : s}$$

$$\text{(SUSP)} \frac{}{\{a \mid \pi(a) \neq \pi'(a)\} \# x : s \vdash \pi x \approx \pi' x : s}$$

## Soundness and Completeness

We write

$$\nabla \vdash_{\mathbb{T}} \bar{a} \# t \approx t' : s$$

if the judgement is provable from the proof rules and the axioms of  $\mathbb{T}$ .

**Soundness** -  $\nabla \vdash_{\mathbb{T}} \bar{a} \# t \approx t' : s \implies \nabla \vDash_{\mathbb{T}} \bar{a} \# t \approx t' : s$  - proved by showing each rule respects satisfaction by a  $\mathbb{T}$ -algebra.

**Completeness** -  $\nabla \vDash_{\mathbb{T}} \bar{a} \# t \approx t' : s \implies \nabla \vdash_{\mathbb{T}} \bar{a} \# t \approx t' : s$  - with ordinary equational logic we build a canonical model out of terms modulo:

$$t \sim t' \text{ iff } \vdash_{\mathbb{T}} t \approx t' : s$$

We then show that satisfaction by this algebra coincides with provability.

In this standard proof variables are essentially treated as new constants.

## Variables in NEL

The variable-free case works much as with equational logic, giving us *ground completeness*:

$$\emptyset \vDash_{\mathbb{T}} \bar{a} \# t \approx t' : s \implies \emptyset \vdash_{\mathbb{T}} \bar{a} \# t \approx t' : s$$

But the analogy between variables and new constants no longer works.

A constant (nullary operation symbol) in NEL has a known finite support, according to the permutation action of  $\text{Op}_{\Sigma}$ .

A variable could have *any* finite support, apart from the finite set of atoms explicitly ruled out by a freshness environment.

**Solution:** Replace variables with constants with supports that are finite but ‘big enough’, given the context.

## Expanding the Signature

Let  $\text{Atom}^{(n)}$  be the nominal set of lists of distinct atoms of length  $n$ .

Let  $\Sigma[c_n : s]$  be the signature defined by

- $\Sigma[c_n : s](\[], s) = \Sigma(\[], s) + \{c_{\vec{a}} \mid \vec{a} \in \text{Atom}^{(n)}\}$
- $\Sigma[c_n : s](\vec{s}, s') = \Sigma(\vec{s}, s')$

So we've added new *atom-parameterised constants* to the signature.

If  $\mathbb{T}$  is a  $\Sigma$ -theory,  $\mathbb{T}[c_n : s]$  is a  $\Sigma[c_n : s]$ -theory with all the same axioms.

## Completeness Proof

Given a judgement

$$\bar{a}' \# x : s' \vdash \bar{a} \# t \approx t' : s$$

Let  $\bar{a}^*$  support  $(\bar{a}, t, t')$  and let  $\vec{a}$  be a list of the atoms in  $\bar{a}^* - \bar{a}'$ . Suppose  $\vec{a}$  has length  $n$ .

$$\begin{array}{l}
 \bar{a}' \# x : s' \quad \vdash_{\mathbb{T}} \bar{a} \# t \approx t' : s \\
 \implies \quad \emptyset \quad \vdash_{\mathbb{T}[c_n:s']} \bar{a} \# t\{c \vec{a}/x\} \approx t'\{c \vec{a}/x\} : s \quad (\text{Easy}) \\
 \implies \quad \emptyset \quad \vdash_{\mathbb{T}[c_n:s']} \bar{a} \# t\{c \vec{a}/x\} \approx t'\{c \vec{a}/x\} : s \quad (\text{Grnd Comp.}) \\
 \implies \quad \bar{a}' \# x : s' \quad \vdash_{\mathbb{T}} \bar{a} \# t \approx t' : s \quad (\text{Hard})
 \end{array}$$

## Further Work

This work provides a springboard to look at **Nominal Universal Algebra** in its own right.

We have shown that free nominal algebras exist, and that the forgetful functor from the category of algebras to  $\mathcal{N}om$  is monadic.

But there is plenty more to look at in this direction: analogues to Birkhoff's theorem, enriched Lawvere theories, etc.

We are also looking to flesh out more examples of NEL-theories, in particular with name-passing calculi such as the  $\pi$ -calculus.

## Related Work

This work is similar to Gabbay & Mathijssen's *nominal algebra* (NA).

NEL has a simpler sort system (lacking abstraction sorts and atom sorts).

NA restricts freshness judgements to decidable side-conditions, so the logic is not complete for such judgements. For example

$$\frac{\nabla \vdash a \# t : s \quad \nabla \vdash t \approx t' : s}{\nabla \vdash a \# u : s}$$

is not valid in NA, while it is provable in NEL where freshness judgements are 'first-class citizens' of the logic.

**Questions?**