Axiomatisation of First-Order Logic

Murdoch J. Gabbay

Joint work with Aad Mathijssen

Second CANS workshop, King's College London UK,
6/12/2005

The issues

This audience is familiar with Nominal techniques. These are based on two things:

- A Fraenkel-Mostowski (FM) sets semantics of α-abstraction.
- Nominal terms as syntax for talking about them.

'Nominal term' is a slightly imprecise term, which I take broadly to be any term language with a term of the form $[a]x$ where a is an atom and x is a variable.

The issues

Nominal terms are great. You can:

- Unify them (and publish a paper).
- Logic-program with them (and publish more papers).
- Implement them in HOL (and publish a paper).
- Rewrite them (and publish more papers).
- Implement rewriting them (and hopefully publish a paper if you haven't already).
- Apologies to nominal termicians whose work I omit.
- You can consider Universal Algebra on nominal terms.

That is the subject of this talk.

Mild warning

I shall not be 100% formal. I miss out a couple of definitions. I assume prior knowledge of Nominal techniques and FM sets.

Sort system

Fix some finite set of base data sorts δ, e.g. $\mathbb{F}$ of formulae and $\mathbb{T}$ of object-level terms.

Fix some finite set of atomic sorts $\mathbb{A}$, e.g. $\mathbb{A}$ the sort of atoms.

Fix some finite set of type-formers tyf each of which has an arity $n > 0$. For example the pair-type $\times$, written infix in grammar of sorts below.

Sorts are defined by:

$$\sigma ::= \delta \quad | \quad \mathbb{A} \quad | \quad \mathsf{tyf}(\overbrace{\sigma, \ldots, \sigma}^{n \text{ times}}) \quad | \quad [\mathbb{A}]\sigma$$

Arities are defined by:

$$\rho ::= (\sigma_1, \ldots, \sigma_n)\delta$$

Sorts vs. types

A sort system guarantees the syntactic well-formedness of a term.

For example multiplication $*$ in the language of arithmetic has arity $(\mathbb{N},\mathbb{N})\mathbb{N}$. A term whose top-level term former is $*$ must have two daughter terms. E.g. $2*2$ is legal syntax and we verify this by checking it has sort $\mathbb{N}$.

A type system guarantees the semantic sanity of a term.

For example multiplication $*$ in the semantics of arithmetic has type $(\mathbb{N}\times\mathbb{N}){\longrightarrow}\mathbb{N}$. In the language of arithmetic, $*$ might be applied to a term which is of type $\mathbb{N}\times\mathbb{N}$, but that term need not have two daughter terms. E.g. $*\Delta 2$ where Δ has type $\mathbb{N}{\longrightarrow}(\mathbb{N}\times\mathbb{N})$ is the diagonal $\lambda x.(x,x)$.

You can tell a sort system, because term-formers can produce only base data types. A type system would allow any σ, not just δ, in the definition of arities above.

Signatures

A signature is:

- A finite set of base data types.
- A finite set of atomic sorts.
- A finite set of term-formers f, to each of which is associated an arity in the sorts mentioning (at most) the base data types and atomic sorts of that signature.

Signature of first-order logic

- $\mathbb{F}$ formulae and $\mathbb{T}$ terms.
- $\mathbb{A}$ atoms.
- - $\bot : \mathbb{F}$ falsity,
  - $\supset: (\mathbb{F}, \mathbb{F})\mathbb{F}$ implication,
  - $\forall : ([\mathbb{A}]\mathbb{F})\mathbb{F}$ universal quantification,
  - $\approx: (\mathbb{T}, \mathbb{T})\mathbb{F}$ (object-level) equality,
  - $sub_\sigma : ([\mathbb{A}]\sigma, \mathbb{T})\sigma$ explicit substitution (for terms, on σ).

Permutations π are finitely-supported bijections on atoms. A bijection is finitely supported when $\pi(a) \neq a$ for some finite set of atoms a, but for all other atoms $\pi(b) = b$.

(So π is 'mostly' the identity.)

Terms are:

$$t ::= a_{\mathbb{A}} \;\mid\; (\pi \cdot X_\sigma)_\sigma \;\mid\; ([a_{\mathbb{A}}]t_\sigma)_{[\mathbb{A}]\sigma} \;\mid\; (\forall t_{[\mathbb{A}]\mathbb{F}})_{\mathbb{F}} \;\mid\; (t_{\mathbb{F}} \supset t_{\mathbb{F}})_{\mathbb{F}} \;\mid\; \bot_{\mathbb{F}} \;\mid\; (t_{\mathbb{T}} \approx t_{\mathbb{T}})_{\mathbb{F}} \;\mid\; sub(t_{[\mathbb{A}]\sigma}, s_{\mathbb{T}})_\sigma.$$

Let t and s be meta-level variables ranging over unknown terms (of unknown sorts). We may drop sort annotations.

We sugar $sub([a]t, s)$ to $t[a \mapsto s]$.

Some example terms

Write $\neg\phi$ for $\phi \supset \bot$, write $\phi \wedge \phi'$ for $\neg(\phi \supset \neg\phi')$, write $\phi \Leftrightarrow \phi'$ for $(\phi \supset \phi') \wedge (\phi' \supset \phi)$, write $\phi \vee \phi'$ for $(\neg\phi) \supset \phi'$, write $\top$ for $\bot \supset \bot$.

Let P, Q be variables of sort $\mathbb{F}$ and T, T' variables of sort $\mathbb{T}$.

1. $\forall[a]\forall[b]P \Leftrightarrow \forall[b]\forall[a]P$.
2. $T \approx T'$.
3. $P[a \mapsto T] \Leftrightarrow P[a \mapsto T']$.
4. $\forall[a]P \Leftrightarrow P$.

Meaning of 'free variables of' with predicate unknowns X.

A freshness $F \equiv a\#t$ is a pair of an atom and a term.

$$\frac{}{a\#b}\,(\#ab) \qquad \frac{a\#t_1 \;\cdots\; a\#t_n}{a\#\mathsf{f}(t_1,\ldots,t_n)}\,(\#\mathsf{f}) \qquad \frac{}{a\#[a]t}\,(\#[]a)$$

$$\frac{a\#t}{a\#[b]t}\,(\#[]b) \qquad \frac{\pi^{-1}\cdot a\#X}{a\#\pi\cdot X}\,(\#X)$$

Let Δ be a set of freshnesses. Write $\Delta \vdash F$ when F follows from Δ (say Δ entails F). Say Δ is primitive when $F' \equiv a\#X$ for all $F' \in \Delta$.

Here f is semi-formal; $\mathsf{f} \in \{\forall, \supset, \bot, \approx, sub\}$.

Axioms and theories

An axiom is a triple $\Delta \vdash t = u$ of a primitive freshness context and two terms.

A theory is a pair of a signature and a finite set of axioms.

Example theories (signatures elided)

The theory CORE:

$$(perm) \quad a, b\#X \rightarrow (a\ b) \cdot X = X$$

Example theories

The theory SUB:

$$(f\mapsto) \quad \mathsf{f}(X_1,\ldots,X_n)[a\mapsto T] = \mathsf{f}(X_1[a\mapsto T],\ldots,X_n[a\mapsto T])$$

$$([b]\mapsto) \quad b\#T \rightarrow ([b]X)[a\mapsto T] = [b](X[a\mapsto T])$$

$$(var\mapsto) \quad a[a\mapsto T] = T$$

$$(X\mapsto) \quad a\#X \rightarrow X[a\mapsto T] = X$$

$$(ren\mapsto) \quad b\#X \rightarrow X[a\mapsto b] = (b\ a)\cdot X$$

Example theories

The theory FOL:

(Props) $P \supset Q \supset P \;=\; \top \qquad \neg\neg P \supset P \;=\; \top$

$$(P \supset Q) \supset (Q \supset R) \supset (P \supset R) \;=\; \top \qquad \bot \supset P \;=\; \top$$

(Quants) $\forall[a]\top = \top \qquad \forall[a]P \supset P[a \mapsto T] \;=\; \top$

$$\forall[a](P \wedge Q) \Leftrightarrow \forall[a]P \wedge \forall[a]Q \;=\; \top$$

$$a\#P \longrightarrow \forall[a](P \supset Q) \Leftrightarrow P \supset \forall[a]Q \;=\; \top$$

Example theories

The theory FOLEQ is as above plus:

(Eq) $$T \approx T' \supset (P[a \mapsto T] \Leftrightarrow P[a \mapsto T']) = \top$$

Other theories eminently possible.

Judgement form of Nominal Algebraic Specifications (NAS)

An NAS judgement is either:

- A triple of a primitive freshness context, an atom, and a term $\Delta \vdash a\#t$.
- A triple of a primitive freshness context and two terms $\Delta \vdash t = u$.

Inductively defined in Natural Deduction style by the freshness rules given earlier, plus:

$$\frac{}{t = t}\,(refl) \qquad \frac{t = u}{u = t}\,(symm) \qquad \frac{t = u \quad u = v}{t = v}\,(tran)$$

$$\frac{t = u}{C[t] = C[u]}\,(cong)$$

$$\frac{\Delta^\pi \sigma}{t^\pi \sigma = u^\pi \sigma}\,(ax_A) \qquad A \equiv \Delta \to t = u$$

$$\begin{array}{c} [a\#X_1, \ldots, a\#X_n] \qquad \Delta \\ \vdots \\ \dfrac{t = u}{t = u}\,(fr) \quad (a \notin t, u, \Delta) \end{array}$$

Example derivation

We derive $[a]X = [b]Y$ from $b\#X$ and $(b\ a) \cdot X = Y$ in CORE:

$$\dfrac{\dfrac{(b\ a) \cdot X = Y}{[b](b\ a) \cdot X = [b]Y}(cong) \qquad \dfrac{b\#X}{b\#[a]X}(\#[]b) \qquad \dfrac{}{a\#[a]X}(\#[]a)}{[a]X = [b]Y}(perm)$$

Write $\Delta \vdash_{\Delta}^{\mathsf{T}} t = u$ when:

- t and u are in the signature of T.
- $t = u$ is derivable from Δ using axioms of T in the derivation.

Conservativity (and other) results require proof-theory

Theorem: FOL is conservative over SUB, which is conservative over CORE.

That is, if $\Delta \vdash^{\mathsf{FOL}} t = u$ and t and u do not mention the term-formers of FOL, then $\Delta \vdash^{\mathsf{SUB}} t = u$.

Similarly if $\Delta \vdash^{\mathsf{SUB}} t = u$ and t and u do not mention explicit substitution, then $\Delta \vdash^{\mathsf{CORE}} t = u$.

But how to prove this? We need proof-theory!

Sequent derivation rules

$$\frac{}{\phi,\ \Phi \ \vdash_{\triangle} \ \Psi,\ \phi}\ (Axiom) \qquad \frac{}{\bot,\ \Phi \ \vdash_{\triangle} \ \Psi}\ (\bot L)$$

$$\frac{\Phi \ \vdash_{\triangle} \ \Psi,\ \phi \qquad \psi,\ \Phi \ \vdash_{\triangle} \ \Psi}{\phi \supset \psi,\ \Phi \ \vdash_{\triangle} \ \Psi}\ (\supset L) \qquad \frac{\phi,\ \Phi \ \vdash_{\triangle} \ \Psi,\ \psi}{\Phi \ \vdash_{\triangle} \ \Psi,\ \phi \supset \psi}\ (\supset R)$$

$$\frac{\phi',\ \Phi \ \vdash_{\triangle} \ \Psi \qquad \phi' \ \vdash_{\triangle}^{\mathsf{SUB}} \ \phi[a{\mapsto}t]}{\forall[a]\phi,\ \Phi \ \vdash_{\triangle} \ \Psi}\ (\forall L)$$

$$\frac{\Phi \ \vdash_{\triangle} \ \Psi,\ \psi \qquad \Delta \ \vdash \ a\#\Phi, \Psi}{\Phi \ \vdash_{\triangle} \ \Psi,\ \forall[a]\psi}\ (\forall R)$$

Sequent derivation rules

$$\frac{\phi', \Phi \vdash \Psi \qquad \phi' \vdash^{\mathsf{SUB}}_{\triangle} \phi''[a \mapsto t'] \qquad \phi \vdash^{\mathsf{SUB}}_{\triangle} \phi''[a \mapsto t]}{t' \approx t, \phi, \Phi \vdash_{\triangle} \Psi} (\approx L)$$

$$\frac{}{\Phi \vdash \Psi, t \approx t} (\approx R)$$

$$\frac{\phi', \Phi \vdash_{\triangle} \Psi \qquad \phi' \vdash^{\mathsf{SUB}}_{\triangle} \phi}{\phi, \Phi \vdash_{\triangle} \Psi} (StructL)$$

$$\frac{\Phi \vdash_{\triangle} \Psi, \psi' \qquad \psi' \vdash^{\mathsf{SUB}}_{\triangle} \psi}{\Phi \vdash_{\triangle} \Psi, \psi} (StructR)$$

We will discuss $\vdash^{\mathsf{SUB}}$ later.

$$\dfrac{\dfrac{\forall[a]\forall[b]X \vdash X \qquad a\#\forall[b]X}{\forall[a]\forall[b]X \vdash \forall[a]X}(\forall R) \qquad b\#\forall[a]\forall[b]X}{\forall[a]\forall[b]X \vdash \forall[b]\forall[a]X}(\forall R)$$

$$\dfrac{\dfrac{\dfrac{}{X \vdash X}(Axiom) \qquad X \vdash^{\mathsf{SUB}} X[b\mapsto b]}{\forall[b]X \vdash X}(\forall L) \qquad \forall[b]X \vdash^{\mathsf{SUB}} (\forall[b]X)[a\mapsto a]}{\forall[a]\forall[b]X \vdash X}(\forall L)$$

Semantics in FOL:

“For all ϕ and ψ, $\forall a.\, \forall b.\, \phi \vdash \forall b.\, \forall a.\, \psi$.”

More of the derivation

$$\dfrac{\dfrac{\dfrac{\dfrac{}{b\#[b]X}\,(\#[]a)}{b\#\forall[b]X}\,(\#\mathsf{f})}{b\#[a]\forall[b]X}\,(\#[]a)}{b\#\forall[a]\forall[b]X}\,(\#\mathsf{f})$$

Another example derivation

$$\dfrac{\dfrac{}{X[a{\mapsto}T'] \vdash X[a{\mapsto}T']}(Axiom) \quad \begin{array}{c} X[a{\mapsto}a][a{\mapsto}T'] \vdash^{\mathsf{SUB}} X[a{\mapsto}T'], \\ X[a{\mapsto}a][a{\mapsto}T] \vdash^{\mathsf{SUB}} X[a{\mapsto}T] \end{array}}{T' \approx T,\ X[a{\mapsto}T] \vdash X[a{\mapsto}T']}(\approx L)$$

Semantics in FOL:

"For all t and t' and ϕ, $t' \approx t,\ \phi[a{\mapsto}t] \vdash \phi[a{\mapsto}t']$."

One more example derivation

$$\dfrac{\dfrac{}{X \vdash_{\triangle} X}(Axiom) \qquad a\#X \vdash a\#X}{X \vdash_{a\#X} \forall[a]X}(\forall R)$$

Semantics in FOL:

"For all ϕ and a, if $a \notin fv(\phi)$ then $\phi \vdash \forall a.\, \phi$."

A theorem:

$$\frac{\Phi \vdash_{\triangle} \Psi, \phi \qquad \phi, \Phi \vdash_{\triangle} \Psi}{\Phi \vdash_{\triangle} \Psi}\,(Cut)$$

Theorem (cut-elimination): Cut is eliminable.

The cut-elimination procedure is almost standard — but details of α-renaming form part of the derivation.

This is one place we need (fr), to generate fresh atoms so we can rename to avoid capture when distributing explicit substitutions under binders. See next slide.

Sequent presentation for $\vdash^{\text{SUB}}$

Write it just $\vdash_{\triangle}$.

$$\frac{}{t \vdash_{\triangle} t}(Axiom) \qquad \frac{t \vdash_{\triangle} u}{C[t] \vdash_{\triangle} C[u]}(Cong)$$

$$\frac{f(t_1[a\mapsto t'],\ldots,t_n[a\mapsto t']) \vdash_{\triangle} u}{f(t_1,\ldots,t_n)[a\mapsto t'] \vdash_{\triangle} u}(fL) \qquad \frac{t \vdash_{\triangle} f(u_1[a\mapsto u'],\ldots,t'_n[a\mapsto u'])}{t \vdash_{\triangle} f(u_1,\ldots,u_n)[a\mapsto u']}(fR)$$

$$\frac{[b](t[a\mapsto t']) \vdash_{\triangle} u \quad \Delta \vdash b\#t'}{([b]t)[a\mapsto t'] \vdash_{\triangle} u}(absL) \qquad \frac{t \vdash_{\triangle} [b](u[a\mapsto u']) \quad \Delta \vdash b\#u'}{t \vdash_{\triangle} ([b]u)[a\mapsto u']}(absR)$$

$$\frac{t \vdash_{\triangle} u \quad \Delta \vdash a,b\#t}{(a\ b)\cdot t \vdash_{\triangle} u}(varL) \qquad \frac{t \vdash_{\triangle} u \quad \Delta \vdash a,b\#u}{t \vdash_{\triangle} (a\ b)\cdot u}(varR)$$

Sequent presentation for $\vdash^{\mathsf{SUB}}$

$$\frac{t \vdash_{\triangle} u}{a[a \mapsto t] \vdash_{\triangle} u}\,(atmL) \qquad \frac{t \vdash_{\triangle} u}{t \vdash_{\triangle} a[a \mapsto u]}\,(atmR)$$

$$\frac{t \vdash_{\triangle} u \quad \Delta \vdash a\#t}{t[a \mapsto t'] \vdash_{\triangle} u}\,(\#L) \qquad \frac{t \vdash_{\triangle} u \quad \Delta \vdash a\#u}{t \vdash_{\triangle} u[a \mapsto u']}\,(\#R)$$

$$\frac{(b\,a) \cdot t \vdash_{\triangle} u \quad \Delta \vdash b\#t}{t[a \mapsto b] \vdash_{\triangle} u}\,(renL) \qquad \frac{t \vdash_{\triangle} (b\,a) \cdot u \quad \Delta \vdash b\#u}{t \vdash_{\triangle} u[a \mapsto b]}\,(renR)$$

Theorem: Cut is admissible for $\vdash^{\mathsf{SUB}}_{\triangle}$.

$$\frac{t \vdash_{\triangle} u \quad u \vdash_{\triangle} v}{t \vdash_{\triangle} v}\,(Cut)$$

Sequent presentation for $\vdash^{\mathsf{CORE}}$

(If you want it)

$$\frac{t \vdash_{\Delta} u}{C[t] \vdash_{\Delta} C[u]}(cong) \qquad \frac{t \vdash_{\Delta, a\#X_1,\ldots,a\#X_n} u}{t \vdash_{\Delta} u}(fr) \quad a \notin t, u$$

$$\frac{(b\ a)\cdot t \vdash_{\Delta} u \quad \Delta \vdash a, b\#t}{t \vdash_{\Delta} u}(permL)$$

$$\frac{t \vdash_{\Delta} (b\ a)\cdot u \quad \Delta \vdash a, b\#u}{t \vdash_{\Delta} u}(permR)$$

Some more theorems:

Theorem: First-order logic corresponds in a natural and formal sense precisely to closed terms (terms mentioning no variables), like $\forall[a](a \approx a)$.

Theorem: Cylindric algebra corresponds in a natural and formal sense precisely to cylindric terms (terms possibly mentioning variables, but not mentioning substitution), like $a \approx b$ (corresponding to 'd_{ab}' in cylindric algebras) or $\neg\forall[a]\neg X$ ('$c_a X$').

Call the sequent logic (at least for FOLEQ; whether we use axiomatic SUB and CORE or sequent versions is up to us) one-and-a-halfth-order logic.

Relation to HOL

Not direct since we can express $a\#t$ and HOL cannot.

Also, suppose $X : o$ and $t : \mathbb{T}$. Then $X[a{\mapsto}t]$ corresponds to ft in HOL where $f : \mathbb{T}{\to}o$. However, $X[a{\mapsto}t][a'{\mapsto}t']$ corresponds to $f'tt'$ where $f' : \mathbb{T}{\to}\mathbb{T}{\to}o$. Similarly $X[a{\mapsto}t][a'{\mapsto}t'][a''{\mapsto}t'']\ldots$

This is type raising.

In one-and-a-halfth-order logic, X remains at sort o throughout and the universal quantification implicit in the use of X allows arbitrary numbers of substitutions.

On the other hand, one-and-a-halfth-order logic is manifestly not (fully) higher-order. For example we can write

$$X \vdash Y$$

meaning in FOL

> "For all formulae ϕ and ψ, $\phi \vdash \psi$."

(A silly but perfectly well-formed judgement.)

In HOL we can write this as $\vdash \forall \phi, \psi.\ \phi \supset \psi$.

However we can also write $\vdash \forall \psi.\ \big((\forall \phi.\ \phi) \supset \psi\big)$.

This is not possible in one-and-a-halfth-order logic: the universal quantification is implicit, and top-level (like ML type quantifiers).
$\forall[X]X \vdash Y$ is not syntax.

Conclusions

One-and-a-halfth-order logic enriches ‘normal FOL’ with predicate unknowns; thus enabling us to reason universally on predicates.

This is like the universal quantification implicit in a variable in a universal algebra judgement $t = u$. And indeed, one-and-a-halfth-order logic arose from an algebraisation of first-order logic.

Conclusions

We have a notion of universal-algebra-with-binding, and along the way have proposed theories for first-order logic with equality (FOLEQ), substitution (SUB), and Nominal Terms (CORE).

I personally am particularly pleased that we can also do proof-theory and reason in a syntax-directed manner, even though the underlying framework is algebraic.

Conclusions

Semantics is interesting.

Should be possible to get semantics just by interpreting abstraction by FM abstraction, permutation by FM permutation, and so on.

An FM sets semantics for FOLEQ has every model locally finite (the Cylindric Algebra version of finite support).

The class of models of FOLEQ in FM sets would consist entirely of locally finite models. Not possible to characterise the class of locally finite models using Universal Algebra (over ZF).

We have demonstrated equivalences with FOLEQ and Cylindric Algebras by syntactic techniques. Writing up a semantics for NAS and thus FOLEQ is a logical next step.

Conclusions

Some other subtleties. For example in SUB we have one $(f\mapsto)$ for each term-former. Why not allow term-former variables in axioms, thus giving some second-order flavour?

Conclusions

For further work, how about. . .

- Two-and-a-halfth-order logic (where you can abstract X; see the NEW calculus of contexts)?
- Implementation and automation?
- Semantics (aside from in FOL)?
- Adding restriction à la Extensions of Nominal Rewriting?

Thanks for listening.