The language of stratified sets, Quine's NF, rewriting, and higher-order logic: A brief tour

Murdoch J. Gabbay

Thanks to Jessica Ryan

8 May 2018

Introduction

This talk is based on two papers:

- The language of stratified sets is confluent and strongly normalising. LMCS, to appear.
  http://www.gabbay.org.uk/papers.html#lanssc
- Consistency of Quine's NF using nominal techniques. Submitted.
  http://www.gabbay.org.uk/papers.html#conqnf

Naïve set theory

Naïve set theory is first-order logic with $=$ and a binary membership relation $\in$ and comprehension terms $\{a \mid \phi\}$.

Syntax of terms and predicates:

$$\begin{aligned} \phi &::= \bot \mid \phi \Rightarrow \phi \mid \forall a.\phi \mid t \in s \mid s = t \\ t &::= a \mid \{a \mid \phi\} \end{aligned}$$

Axioms are standard for FOL with equality, along with:

- Extensionality $\forall a, b.(\forall c.(c \in a \Leftrightarrow c \in b)) \Rightarrow a = b$.
- Comprehension $t \in \{a \mid \phi\} \Leftrightarrow \phi[a{:=}t]$.

Russell's paradox

Naïve set theory is inconsistent. Define the Russell set

$$R = \{a \mid a \notin a\}.$$

Then Russell observed that

$$R \in R \Leftrightarrow R \notin R,$$

from which we conclude

$$\bot.$$

Oops.

(n-fold Russell)

Incidentally, this paradox is quite robust. For instance, define $x \in^n y$ for $n \geq 1$ by

- $x \in^1 y$ when $x \in y$ and
- $x \in^{n+1} y$ when $\exists x'.(x \in x' \wedge x' \in^n y)$.

Then define the *n*-fold Russell set

$$R^n = \{a \mid a \notin^n a\}.$$

Then it is possible to prove that

$$R^n \in^n R^n \Leftrightarrow R^n \notin^n R^n.$$

Avoiding Russell's paradox

Back in the 1930s, mathematical foundations were of interest to philosopher mathematicians. This inconsistency was deeply annoying to a select group.

Nowadays foundations are big business. For any interesting formal specification, verification, or programming language, we need a foundation for mathematics that won't obviously derive $\perp$. We cannot base the world on naïve sets.

Solutions were developed:

- Zermelo set theory. Restrict to bounded comprehension $\{a \in s \mid \phi\}$.
- Higher-order logic: simply-typed λ-calculus with *bool* and *nat*.
- Quine's NF. Restrict to stratifiable comprehension.

Stratifiability

A predicate ϕ is stratifiable when there is a way to assign levels in $\mathbb{N} = \{0, 1, 2, \dots\}$ to variables and terms appearing in ϕ such that:

- If $\{a \mid \phi'\}$ appears in ϕ then $\mathit{level}(\{a \mid \phi'\}) = \mathit{level}(a)+1$.
- If $t \in s$ appears in ϕ then $\mathit{level}(s) = \mathit{level}(t) + 1$.
- If $s = t$ appears in ϕ then $\mathit{level}(s) = \mathit{level}(t)$.

Quine's NF permits a comprehension $\{a \mid \phi\}$ provided ϕ is stratifiable.

Expressivity of Quine's NF

The universal set

$$\mathcal{U} = \{a \mid \top\}$$

is stratifiable. So the universe of all elements is a set. And yes, $\mathcal{U} \in \mathcal{U}$; the universe is an element of itself.

This is fine: sets membership is not well-founded.

The cardinality $\mathbf{2}$

$$\mathbf{2} = \{a \mid \exists b, c. b \neq c \wedge \forall a'.(a' \in a \Leftrightarrow (a' = b \vee a' = c))\}$$

is a set. This is the set of all two-element sets.

Similarly for $\mathbf{3}$, $\mathbf{4}$, and so forth.

Indeed we can form **Card** the set of all sets of equipollent (have-the-same-cardinality) sets. This is the set of all cardinalities and is itself a set!

Stratification vs stratifiability

Let the language of stratified sets (LSS) be first-order logic with $=$ and $\in$ and comprehension $\{a \mid \phi\}$ where variables are indexed by $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Define $level(\{a \mid \phi\}) = level(a)+1$ as usual.

Call ϕ stratified when if $t \in s$ appears in ϕ then $level(s) = level(t) + 1$.

NF insists on stratifiability; LSS insists on stratification.

LSS can express $\mathbf{2}^i$ for every $i \geq 3$ as follows:

$$\mathbf{2}^i = \{a^{i\text{-}1} \mid \exists b^{i\text{-}2}, c^{i\text{-}2}.b \neq c \wedge \forall (a')^{i\text{-}3}).(a' \in a \Leftrightarrow (a'{=}b \vee a'{=}c))\}$$

Then $level(\mathbf{2}^i) = i$ and there's a copy of 'the cardinality 2' at every level above 2.

Translation LSS $\rightarrow$ HOL

On types $\mathbb{N} = \{0, 1, 2, \dots\}$ we define:

- $hol(0) = nat$
- $hol(i{+}1) = hol(i) \rightarrow bool$

We might write $hol(i) = powerset^i(nat)$.

On predicates and terms we define:

- $hol(a^i) = a$ for some appropriate HOL variable $a : hol(i)$
- $hol(\{a \mid \phi\}) = \lambda a.hol(\phi)$
- $hol(t \in s) = s\ t$
- $hol(\forall a.\phi) = \forall\ hol(\phi)$
- $hol(\phi \Rightarrow \phi') = \ \Rightarrow hol(\phi)\ hol(\phi')$
- $hol(\bot) = \bot$

Translation LSS to HOL syntax

So LSS can be viewed as a syntactic subsystem of Higher-Order Logic.

- Comprehension becomes λ-abstraction and $\beta\eta$. E.g. $t \in \{a \mid \phi\} \Leftrightarrow \phi[a{:=}t]$ is just $(\lambda a.hol(\phi))hol(t) = hol(\phi)[a{:=}hol(t)]$ or more briefly $(\lambda a.\phi)t = \phi[a{:=}t]$.
- Sets membership becomes application.
- Extensionality becomes functional extensionality.

To be clear: Quine's NF is not a sub-logic of HOL ...

LSS $\rightarrow$ HOL syntax

Quine's NF is not a sub-logic of HOL.

This is because NF's stratifiability condition engenders — in translation to the stratified syntax LSS — an additional typical ambiguity axiom, that if ϕ is a closed predicate then:

$$\phi \Leftrightarrow \phi^+$$

where ϕ^+ is obtained by increasing the level of every variable in ϕ by 1.

Consider $\phi = \{\mathbf{3}^i, \mathbf{4}^i\} \in \mathbf{2}^{i+2}$ (should be valid). Then

$$\phi^+ = \{\mathbf{3}^{i+1}, \mathbf{4}^{i+1}\} \in \mathbf{2}^{i+3}.$$

NF $\not\to$ HOL

Unfortunately $hol(i+1)$ is larger than $hol(i)$ by a Gödel diagonalisation argument.

So the obvious translation of LSS into HOL, while revealing, does not obviously imply consistency of NF.

Far from it! This has been an open problem for nearly 90 years.

I constructed a claimed model of NF in my second paper cited above.

Language of Stratified Sets

Let us return to the Language of Stratified Sets. There are interesting things to say just about this system.

Theorem 1: LSS with rewrite $t \in \{a \mid \phi\} \to \phi[a{:=}t]$ is confluent.

Theorem 2: LSS with same rewrite is strongly normalising.

Proof: Either

- by direct calculations (see my first paper cited above), or
- by the translation *hol* to HOL, proving that *hol* commutes properly through substitution and reduction (e.g. $hol(\phi[a{:=}t]) = hol(\phi)[a{:=}hol(t)])$ — and then using confluence and strong normalisation for simply-typed λ-calculus.

The direct confluence and strong normalisation proofs for LSS are somewhat simpler than those for the full untyped λ-calculus.

LSS normal forms

Normal forms of LSS are defined as follows:

$$\begin{aligned} \phi &::= \bot \mid \phi \Rightarrow \phi \mid \forall a.\phi \mid t \in a \\ s, t &::= a \mid \{a \mid \phi\}. \end{aligned}$$

The important part is $t \in a$; if we have $t \in \{a \mid \phi\}$ then this is not a normal form.

LSS normal forms form what I call a sigma-algebra, meaning a nominal algebra for substitution. The substitution action on normal forms is quite attractive, in a baroque kind of way.

NF is confluent and strongly normalising

The language of NF stratifiable syntax; like LSS's stratified syntax, but variables are not assigned a priori levels

$$\begin{aligned} \phi &::= \bot \mid \phi \Rightarrow \phi \mid \forall a.\phi \mid t \in s \\ s, t &::= a \mid \{a \mid \phi\} \qquad \phi \text{ stratifiable.} \end{aligned}$$

Theorem: Stratifiable syntax is confluent and strongly normalising under the β-rewrite $t \in \{a \mid \phi\} \to \phi[a{:=}t]$ and its normal forms are a sigma-algebra.

Proof: choose a stratification, translate to LSS, and reduce there.

Conclusions

NF is a nice system in which we can express nice things. I find it a refreshing change of perspective from ZF and HOL.

Though long known, there remain elementary things to say about it, such as to study its theory of rewriting.

(I claim that) NF has a model and is consistent.