Nominal Algebraic Specifications

Murdoch J. Gabbay

Joint work with Aad Mathijssen

November 2005

Universal Algebra

Algebra is great, because it is so simple. There is only one judgement form, $t = u$ (t is equal to u).

Equality is an equivalence relation:

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

Also, equal elements *are* equal, and thus interchangeable:

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

Universal Algebra

A theory is just a finite set of equalities.

A model of algebra is just a set with associated functions, one for each function symbol in the language of the terms between which we asserted the equalities, such that the equalities asserted *are* valid.

A classic example is the theory of groups. Three function symbols: $\cdot$ composition, 1 the unit, and -$^{-1}$ inverse. Axioms are:

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z \qquad x \cdot 1 = 1 \cdot x = x \qquad x \cdot x^{-1} = x^{-1} \cdot x = 1$$

You could easily come up with plausible axioms for rings and fields.

Binary term-formers $\wedge$ and $\vee$, unary term-formers $\neg$, constants 0 and 1. Axioms are:

$$
\begin{array}{rl}
x \vee y = y \vee x & x \wedge y = y \wedge x \\
x \vee (y \vee z) = (x \vee y) \vee z & x \wedge (y \wedge z) = (x \wedge y) \wedge z \\
x \vee x = x & x \wedge x = x \\
x = x \vee (x \wedge y) & x = x \wedge (x \vee y) \\
x \wedge 0 = 0 \qquad x \vee 1 = 1 & x \wedge \neg x = 0 \qquad x \vee \neg x = 1
\end{array}
$$

The simplest model of this is the two-element set $\{0, 1\}$. 0 is 0, 1 is 1, $\neg$ is 'swap 0 and 1', $\wedge$ is min and $\vee$ is max.

Theorems of the model theory of Universal Algebra state that, up to putting models together like lego (cross product, basically), this is the *only* model.

Typical theorem of Universal Algebra

My favourite algebraic theory has terms t and u in it of which I can prove $t = u$. I know by [Theorem] that any algebra satisfying $t = u$ has a certain property of its models. Therefore, this favourite model of my theory has that property.

Thus we have gone from properties of (a very simple logic) to properties of (possibly very complex) sets.

More generally, the form of a logical assertion dictates under what operations on models of that assertion the assertion remains valid. The simpler the assertion, the more things we can do to the model. The very simplicity and atomicity of the assertion $t = u$ gives it great power.

Oh yes, and by the way. . .

. . . algebra is good for theorem-provers as well, because nearly every theorem-prover has an equality, and the validity of an equality depends only on the form of t and u, in particular on whether $t = u$ can be derived.

Thus the algorithmics of proving $t = u$ is reduced to the algorithmics of using the axioms to rewrite t to u.

Cylindric algebra (CA)

Variables are p, q, r. Binary term-formers $\wedge$ and $\vee$. Unary term-formers $\neg$ and c_i for $i \in \mathbb{N}$. Constants d_{ij} for $i, j \in \mathbb{N}$, also 0 and 1.

$$p \wedge 0 = 0 \qquad p \vee 0 = p \qquad p \wedge 1 = p \qquad p \vee 1 = 1$$

$$p \wedge \neg p = 0 \qquad p \vee \neg p = 1 \qquad c_i 0 = 0 \qquad p \wedge c_i p = c_i p$$

$$c_i(p \wedge c_i q) = c_i p \wedge c_i q \qquad d_{ii} = 1$$

$$d_{ik} = c_j(d_{ij} \wedge d_{jk}) \qquad c_i(d_{ij} \wedge p) \wedge c_i(d_{ij} \wedge \neg p) = 0.$$

Isn't maths great.

In other terms

Choose some countably infi nite set $a, b, c, \ldots$ in bijection with $\mathbb{N}$. Write:

- $\exists a$ for c_a.
- $a \approx b$ for d_{ab}.

Then the axioms become:

$$P \wedge 0 = 0 \qquad P \vee 0 = P \qquad P \wedge 1 = P \qquad P \vee 1 = 1$$

$$P \wedge \neg P = 0 \qquad P \vee \neg P = 1 \qquad \exists a.0 = 0 \qquad P \wedge \exists a.P = \exists a.P$$

$$\exists a.(P \wedge \exists a.Q) = \exists a.P \wedge \exists a.Q$$

$$(a \approx a) = 1$$

$$(a \approx c) = \exists b.((a \approx b) \wedge (b \approx c))$$

$$\exists a.((a \approx b) \wedge P) \wedge \exists a.((a \approx b) \wedge \neg P) = 0.$$

Notes

- P, Q represent *unknown predicates*.
- There is no term language — the only terms are the ‘variable symbols’ a, b, c.
- $\approx$ is a formal equality symbol inside the language; that’s one reason we wrote it d_{ab} originally.

Nominal Algebraic Specifi cations (NAS) sorts

Sorts serve to partition the model into distinct sets with functions between them (rather than just one set with functions to itself, as is the case for groups.

Fix base sorts $\mathbb{F}$ of formulae and $\mathbb{T}$ of terms. Fix an atomic sort $\mathbb{A}$.

Sorts τ and arities ρ are defi ned by the following grammars:

$$\tau ::= \delta \mid \mathbb{A} \mid [\mathbb{A}]\delta \qquad \rho ::= (\tau_1, \ldots, \tau_n)\delta$$

Here n may be zero. We indicate sorts and arities with subscripts.

Let $a_{\mathbb{A}}, b_{\mathbb{A}}, c_{\mathbb{A}}, \ldots$ and $X_\tau, Y_\tau, Z_\tau, \ldots$ be disjoint countably infi nite sets of formal symbols we call atoms and variables respectively.

Let the $a, b, c, \ldots$ from cylindric algebras correspond to atoms. Let the p, q, r from cylindric algebras correspond to variables $X_{\mathbb{F}}, Y_{\mathbb{F}}, Z_{\mathbb{F}}$.

We have to formally define what a term is — we did not do it before, but the definition was still lurking in the background. A term is still a term.

Term-formers have arities as shown in subscripts:

$$\bot_{\mathbb{F}} \quad \supset_{(\mathbb{F},\mathbb{F})\mathbb{F}} \quad \forall_{([\mathbb{A}]\mathbb{F})\mathbb{F}} \quad \mathsf{var}_{(\mathbb{A})\mathbb{T}} \quad \sigma_{([\mathbb{A}]\mathbb{F},\mathbb{T})\mathbb{F}} \quad \approx_{(\mathbb{T},\mathbb{T})\mathbb{F}}$$

(Equality comes later.)

Terms t, u, v, w are:

$$t \ ::= a_{\mathbb{A}} \mid (\pi \cdot X_\tau)_\tau \mid [a_{\mathbb{A}}]t_\tau \mid (\mathsf{f}_{(\tau_1,\ldots,\tau_n)\delta}(t^1_{\tau_1},\ldots,t^n_{\tau_n}))_\delta$$

$(\pi \cdot X_\tau)_\tau$ is a moderated variable. π is a *finitely supported permutation of atoms*, i.e. a bijection on atoms such that for finitely many atoms $\pi(a) \neq a$ (possibly none), and for all the others $\pi(a) = a$.

Without sorts: $t \ ::= a \mid \pi \cdot X \mid [a]t \mid \mathsf{f}(t^1,\ldots,t^n)$.

Here $\mathsf{f} \in \{\bot,\ \supset,\ \forall,\ \mathsf{var},\ \sigma,\ \approx\}$.

A freshness assertion is a pair $a\#t$ of an atom and a term. Here is how we derive them:

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

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

$$\begin{array}{c} [a\#t_1,\ldots,a\#t_n] \\ \vdots \\ \dfrac{E}{E} \end{array}(Fr) \quad (a \notin E, t_1,\ldots,t_n)$$

The condition on (Fr) expresses that atom a does not occur in the equation E and any of the terms $t_1,\ldots,t_n$.

A freshness context Δ is a fi nite set $\{a^1\#X^1,\ldots,a^n\#X^n\}$.

- Call $t_\tau = u_\tau$ a equality E.
- Call a triple $\Delta \to t = u$ an axiom. If $\Delta = \emptyset$ we may write just $t = u$.

Here are our axioms!

The core theory CORE*.*

$$(var) \quad a, b\#X \to (a\ b) \cdot X = X$$

Explicit substitution SUB*.*

$$\mathsf{f}(Z_1, \ldots, Z_n)[a \mapsto X] = \mathsf{f}(Z_1[a \mapsto X], \ldots, Z_n[a \mapsto X])$$

$$b\#X \to ([b]Y)[a \mapsto X] = [b](Y[a \mapsto X])$$

$$\mathsf{var}(a)[a \mapsto X] = X \qquad a\#Z \to Z[a \mapsto Y] = Z$$

$$Z[a \mapsto \mathsf{var}(a)] = Z$$

More axioms

(Props) $P \supset Q \supset P \ = \ \top \quad \neg\neg P \supset P \ = \ \top$

$$(P \supset Q) \supset (Q \supset R) \supset (P \supset R) \ = \ \top \quad \bot \supset P \ = \ \top$$

(Quants) $\forall[a]\top = \top \qquad \forall[a]P \supset P[a{\mapsto}Q] \ = \ \top$

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

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

(Equal) $X{\approx}X = \top \qquad X{\approx}Y \supset P[a{\mapsto}X] \Leftrightarrow P[a{\mapsto}Y] = \top.$

Derivability for equalities

Define a notion of derivability on equalities as follows:

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

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

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

Here $C[\text{-}]$ is 'a term with a hole'. -$^{\pi}$ denotes the term obtained by *actually* applying π to that term.

Some theorems:

- First-order logic as we know it corresponds to closed terms of our NAS theory, up to provable equality.
- Cylindric algebra corresponds to cylindric terms; possibly open terms of our NAS theory which do not mention explicit substitution or permutation (plus other minor conditions), up to provable equality.

'Closed' means 'mentions no variables'. This is where people come unstuck. Importantissimo to distinguish between:

- Object-level variable symbols a, b, c and object-level equality $\approx$ and abstraction $[a]$- and explicit substitution $t[a \mapsto u]$ and
- meta-level variable symbols X, Y, Z, meta-level equality $=$, and meta-level substitution $C[t]$.

How do we set about proving something like this? First, set up the translations. They are pretty obvious really, we give just two examples:

- $\forall a.\ a = a$ in FOL maps to $\forall[a](\mathsf{var}(a)\approx\mathsf{var}(a))$ in (this particular theory of) NAS.
- Conversely a closed term, e.g. $(\mathsf{var}(a)\approx\mathsf{var}(b))[a\mapsto\mathsf{var}(b)]$ maps to $b = b$ in FOL.
- The translation between cylindric algebras and NAS is direct. c_a corresponds to $\neg\forall[a]\neg$ and d_{ab} to $\mathsf{var}(a)\approx\mathsf{var}(b)$. Variables $P_{\mathbb{F}}$ correspond with variables P.

Problem

The next step is to prove by induction on NAS derivations/ FOL derivations/ CA derivations that these transations preserve provable equivalence and are self-inverse up to provable equality.

The diffi culty is $\dfrac{t = u \quad u = v}{t = v}\,(tran)$.

Oh it looks so innocent. But think about it:

Our characterisation of FOL and CA in NAS was syntactic. But u appears above the line; it need be neither closed, nor cylindric, and it may exploit the full complexity of the NAS theory of fi rst-order logic to be equal to t and v.

“$(tran)$ is not syntax-directed.”

Beautiful solution

Write ϕ and ψ for terms of sort $\mathbb{F}$. Write Φ and Ψ for finite sets of $\{\phi_1, \ldots, \phi_j\}$ and $\{\psi_1, \ldots, \psi_k\}$. Write

$$\Phi \vdash_{\Delta} \Psi \qquad \text{for} \qquad \Delta \vdash (\phi_1 \wedge \cdots \wedge \phi_j \supset \psi_1 \vee \cdots \vee \psi_k) = \top.$$

Then we prove that the following sequents are justified in NAS (theory of FOL with equality)...

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

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

$$\frac{\Phi\ \vdash_{\Delta}\ \phi,\ \Psi \quad \Delta\ \vdash\ a\#\Phi,\Psi}{\Phi\ \vdash\ \forall a.\phi,\Psi}(\forall R) \qquad \frac{\Phi,\ \phi'\ \vdash_{\Delta}\ \Psi \quad \Delta\ \vdash_{\mathsf{SUB}}\ \phi' = \phi[a\mapsto t]}{\Phi,\ \forall a.\phi\ \vdash\ \Psi}(\forall L)$$

$$\frac{\Phi,\ \phi\ \vdash_{\Delta}\ \psi,\ \Psi \quad \Delta\ \vdash_{\mathsf{SUB}}\ \phi = \phi' \quad \Delta\ \vdash_{\mathsf{SUB}}\ \psi = \psi'}{\Phi,\ \phi'\ \vdash_{\Delta}\ \psi',\ \Psi}(Struct)$$

$$\frac{\Phi\ \vdash\ \phi,\ \Psi \quad \Phi,\ \phi\ \vdash\ \Psi}{\Phi\ \vdash\ \Psi}(Cut)$$

Beautiful solution

That's pretty easy. But we also show that any valid derivation in that sequent system has a cut-free derivation.

All our results follow, because now induction on derivations is syntax-directed.

Conclusions

Algebra is a useful tool. However, it is limited in its treatment of binding.

By extending universal algebra with *stuff* for binding we have been able to give an interesting algebraisation of fi rst-order logic, and one which follows the usual sequent-style presentation *so closely* that we can use techniques from sequent presentations (cut-elimination) to prove results about the algebraic system.

I claim that the model theory of universal algebra is valid for NAS, in the universe of Fraenkel-Mostowski sets. I have not yet proved this, but supporting evidence is a sound and complete semantics for Fresh Logic in FM sets (see [Gabbay 'Fresh Logic']). Fresh Logic is (pretty much) a strict superset of NAS.