Why Universal Algebra needs Inductive, Dependent Types

William DeMeo

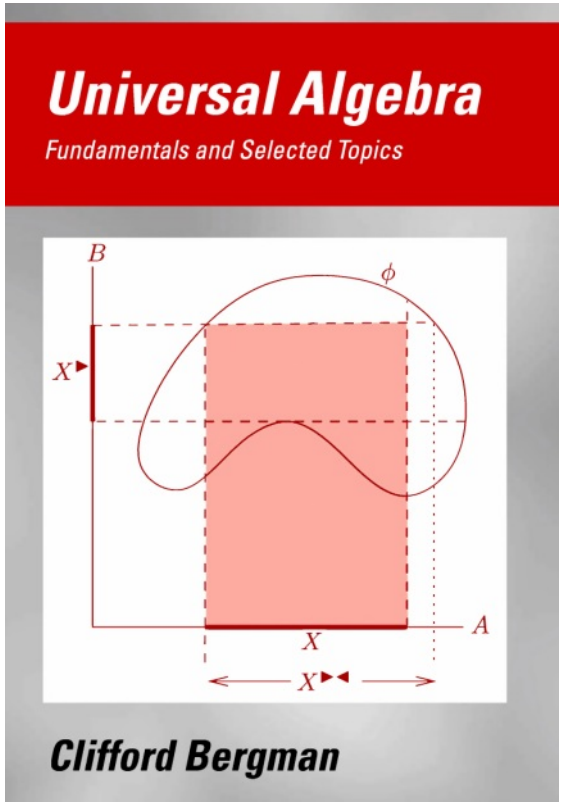
OPLSS 2018

Main References

- The Math-classes Coq library
  Spitters & vanDenWeegan (2010)

- Venanzio Capretta's Thesis
  (Coq) (2000)

- LEAN
  leanprover.github.io



(Algebraic) STRUCTURES

- **signature** $\sigma = (C, F, R, \rho)$ where

  C = a set of constant symbols
  F = " " operation symbols
  R = " " relation symbols

  $\rho : F + R \to \mathbb{N}$, arity function

- **structure of type σ**

  $\mathcal{A} = \langle A, \{C^{\mathcal{A}}, F^{\mathcal{A}}, R^{\mathcal{A}}\}\rangle$ where A = a set of "elements" of the structure, (aka the "universe" or "carrier")

  Typically, for universal algebra, $R = \emptyset$, and F includes C as the set of nullary (0-ary) operation symbols.

(i.e. we tend to focus on "algebras" of the form $\mathcal{A} = \langle A, F^{\mathcal{A}}\rangle$)

SUBSTRUCTURES

Given a set of elements in an algebra we are often interested in the smallest subuniverse containing those elements.

Definition 1. Let $\mathbf{A}$ be an algebra and $X \subseteq A$. The *subuniverse of* $\mathbf{A}$ *generated by* X is $\mathrm{Sg}^{\mathbf{A}}(X) = \bigcap \{ U \in \mathrm{Sub}(\mathbf{A}) : X \subseteq U \}$.

Theorem 1. *Let* $\mathbf{A} = \langle A, F \rangle$ *be an algebra and* $X \subseteq A$. *Define, by recursion on* n, *the sets* X_n *by:*

$$X_0 = X;$$
$$X_{n+1} = X_n \cup \{ f(a_1, \ldots, a_k) : a_1, \ldots, a_k \in X_n, f \in F, \text{ and } k = \mathrm{rank}\, f \}.$$

Then $\mathrm{Sg}^{\mathbf{A}}(X) = \bigcup_{n \in \omega} X_n$.

SUBSTRUCTURES

Theorem 1. *Let* $\mathbf{A} = \langle A, F \rangle$ *be an algebra and* $X \subseteq A$. *Define, by recursion on* n, *the sets* X_n *by:*

$$X_0 = X;$$
$$X_{n+1} = X_n \cup \{ f(a_1, \ldots, a_k) : a_1, \ldots, a_k \in X_n, f \in F, \text{ and } k = \operatorname{rank} f \}.$$

Then $\operatorname{Sg}^{\mathbf{A}}(X) = \bigcup_{n \in \omega} X_n$.

Proof. Let $Y = \bigcup_{n \in \omega} X_n$. Clearly $X_n \subseteq Y \subseteq A$, for every $n \in \omega$. In particular $X = X_0 \subseteq Y$. Let us show that Y is a subuniverse of $\mathbf{A}$. Let f be a basic k-ary operation and $a_1, \ldots, a_k \in Y$. From the construction of Y, there is an $n \in \omega$ such that $a_1, \ldots, a_k \in X_n$. From its definition, $f(a_1, \ldots, a_k) \in X_{n+1} \subseteq Y$. Thus Y is a subuniverse of $\mathbf{A}$ containing X. By Definition 1.13, $\operatorname{Sg}^{\mathbf{A}}(X) \subseteq Y$.

For the opposite inclusion, it is enough to check, by induction on n, that $X_n \subseteq \operatorname{Sg}^{\mathbf{A}}(X)$. Well, $X_0 = X \subseteq \operatorname{Sg}(X)$ from its definition. Assume that $X_n \subseteq \operatorname{Sg}(X)$. If $b \in X_{n+1} - X_n$ then $b = f(a_1, \ldots, a_k)$ for a basic k-ary operation f and $a_1, \ldots, a_k \in X_n$. But $a_1, \ldots, a_k \in \operatorname{Sg}(X)$ and since this latter object is a subuniverse, $b \in \operatorname{Sg}(X)$ as well. □

CLONES

• Projections

Let A be a set. For every natural number n let $\mathrm{Op}_n(A)$ denote the set of all n-ary operations on A. Put another way, $\mathrm{Op}_n(A) = A^{(A^n)}$. Let $\mathrm{Op}(A) = \bigcup_{n\in\omega} \mathrm{Op}_n(A)$ be the set of all operations on A. For any $k \leq n$ there is an n-ary operation $p^n_k(x_1, \ldots, x_n) = x_k$, called the *$k$-th projection operation*.

• Generalized composition

Let n and k be natural numbers, and suppose that $f \in \mathrm{Op}_n(A)$ and $g_1, \ldots g_n \in \mathrm{Op}_k(A)$. Then we define a new k-ary operation $f[g_1, \ldots, g_n]$ by

$$(x_1, x_2, \ldots, x_k) \mapsto f\big(g_1(x_1, \ldots, x_k), \ldots, g_n(x_1, \ldots, x_k)\big)$$

called the *generalized composite* of f with $g_1, \ldots, g_n$. Note that, unlike the ordinary composition of unary operation, the generalized composite only exists when all of the ranks match up correctly.

CLONES

Just as the set of unary operations forms a monoid under the operation of composition, we can form a kind of algebraic structure whose elements are members of $\mathrm{Op}(A)$ with the operation of generalized composition.

partial!

- **Definition 2.** Let A be a nonempty set. A *clone* on A is a subset $\mathcal{C}$ of $\mathrm{Op}(A)$ that contains all projection operations and is closed under generalized composition.

- **Example**

  - $\mathrm{Op}(A)$ and $\mathrm{Proj}(A) = \{ p_k^n : 1 \leq k \leq n \in \omega \}$ are clones on any set A.

  - The set $\mathcal{E}(A)$ of all idempotent operations on A is a clone. Recall that an operation f is *idempotent* if $f(x, x, \ldots, x) = x$ for all x.

  - Let $\langle P, \leq \rangle$ be a poset. The set of all isotone operations is a clone on P. An operation f is *isotone* if $x_i \leq y_i$ for $i \leq n$ implies $f(x_1, x_2, \ldots, x_n) \leq f(y_1, \ldots, y_n)$.

CLONES

As a rule, a clone is a very complicated object, containing operations of every rank. Unlike the above examples, most clones can not be described easily as "the set of all f such that blah-blah-blah." It is a major challenge just to find techniques for characterizing clones.

Post [Pos41] proved in 1941 that the lattice of clones on a two-element set is countable. By contrast, if $|A| > 2$ then A has uncountably many clones (Janov and Mucnik [JM59], 1959; and Hulanicki and Świerczkowski [HŚ60], 1960). For infinite sets A, the lattice of clones seems to be so complicated that almost nothing is known about it.

i.e. inductive

As always, we seek a "bottom-up" description of the members of $\mathrm{Clo}(F)$. By thinking of a clone as a kind of algebra it is clear that a description analogous to Theorem 1 ought to be possible. But recall that function composition, even generalized composition, is associative. This makes it possible to provide a slightly slicker formulation.

CLONES

Theorem 2. *Let A be a set and F a set of operations on A. Define*

$$\begin{aligned} F_0 &= \mathrm{Proj}(A); \\ F_{n+1} &= F_n \cup \big\{ f[g_1, \ldots, g_k] : f \in F,\ k = \mathrm{rank}\, f \\ &\qquad \text{and } g_1, \ldots, g_k \in F_n \cap \mathrm{Op}_m(A),\ \text{some } m \in \omega \big\}, \quad \textit{for } n \in \omega. \end{aligned}$$

Then $\mathrm{Clo}^A(F) = \bigcup_n F_n$.

CLONES

Proof. Let $\overline{F} = \bigcup_n F_n$. It is easy to argue by induction that every $F_n \subseteq \mathrm{Clo}(F)$. Thus $\overline{F} \subseteq \mathrm{Clo}(F)$. For the converse, we must show that $\overline{F}$ is a clone containing F. Since $F_0 \subseteq \overline{F}$, we see that $\overline{F}$ contains the projection operations. Also, for any k-ary operation $f \in F$ we have $f = f[p_1^k, p_2^k, \ldots, p_k^k] \in F_1 \subseteq \overline{F}$. We are reduced to showing that $\overline{F}$ is closed under generalized composition. This follows from the following claim.

Claim. If $f \in F_n$ is k-ary and if $g_1, \ldots, g_k \in F_m$ are all of the same rank, then $f[g_1, \ldots, g_k] \in F_{n+m}$.

Proof. We prove the claim by induction on n. If $n = 0$ then f is a projection, so $f[g_1, \ldots, g_k] = g_i \in F_{0+m}$ for some $i \leq k$. So assume the claim holds for n and that $f \in F_{n+1} - F_n$. From the definition, there are operations $f_1 \in F$ of rank t and $h_1, \ldots, h_t \in F_n$ such that $f = f_1[h_1, \ldots, h_t]$. Note that the rank of each h_i must be equal to the rank of f, namely k. By the induction hypothesis, for each $i \leq k$, $h_i' = h_i[g_1, \ldots, g_k] \in F_{n+m}$. Applying the definition, $f_1[h_1', \ldots, h_t'] \in F_{n+m+1} = F_{(n+1)+m}$. Since

$$f_1[h_1', \ldots, h_t'] = f_1[h_1[\mathbf{g}], \ldots, h_t[\mathbf{g}]] = f[\mathbf{g}]$$

the claim is proved. □

TERMS

Recall that a similarity type is a function $\rho\colon \mathcal{F} \to \omega$ where the members of the index set $\mathcal{F}$ are called the *operation symbols* of ρ. If f is an operation symbol and $\mathbf{A}$ is an algebra of type ρ, we usually write $f^{\mathbf{A}}$ to denote the basic operation on A indexed by f.

we wish to extend the idea of operation symbol to include formal objects that correspond, in any given algebra, to the term operations on the algebra.

Fix a similarity type $\rho\colon \mathcal{F} \to \omega$, and let X be a set disjoint from $\mathcal{F}$. The elements of X are called *variables*. For every $n \in \omega$, let $\mathcal{F}_n = \rho^{-1}\{n\}$ i.e., the set of n-ary operation symbols. By a *word* on $X \cup \mathcal{F}$ we mean a nonempty, finite sequence of members of $X \cup \mathcal{F}$. We denote the concatenation of sequences by simple juxtaposition.

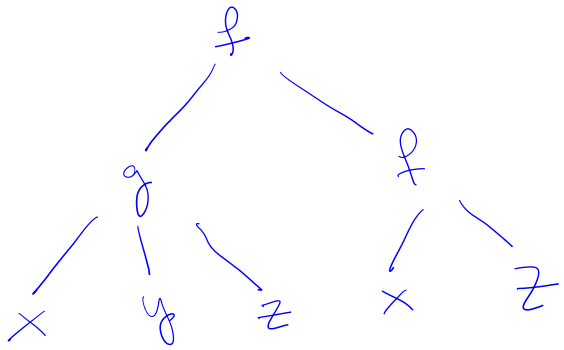
TERMS

A complicated term is a sequence consisting of several operation symbols interspersed with variables. We use the notation $t(x_1, \ldots, x_n)$ to denote a term whose variables are among $x_1, \ldots, x_n$. For example, if f is a binary term and g is ternary, then the term

$$f(g(x, y, z), f(x, z)) \text{ which is formally } \langle f, g, x, y, z, f, x, z \rangle$$

might be denoted $t(x, y, z)$ if we don't care to indicate the exact form of the term.

$t(x\,y\,z) = f(g(x\,y\,z), f(x, z))$



TERMS

Definition 3. Let $\rho\colon \mathcal{F} \to \omega$ be a similarity type and X a set disjoint from $\mathcal{F}$. We define, by recursion on n, the sets T_n of words on $X \cup \mathcal{F}$ by

$$T_0 = X \cup \mathcal{F}_0$$
$$T_{n+1} = T_n \cup \{\, f s_1 s_2 \dots s_k : f \in \mathcal{F},\ k = \rho(f) \text{ and } s_1, \dots, s_k \in T_n \,\}.$$

Finally, we define $T_\rho(X) = \bigcup_{n\in\omega} T_n$, called the set of *terms of type ρ over X*.

Term height

Referring again to Definition 3., if w is a term, we define $|w|$ to be the least n such that $w \in T_n$, called the *height* of w. The height is a useful index for recursion and induction.

A Common Theme

- Substructures

Theorem 1. *Let $\mathbf{A} = \langle A, F \rangle$ be an algebra and $X \subseteq A$. Define, by recursion on n, the sets X_n by:*

$$X_0 = X;$$
$$X_{n+1} = X_n \cup \{ f(a_1, \ldots, a_k) : a_1, \ldots, a_k \in X_n, f \in F, \text{ and } k = \operatorname{rank} f \}.$$

Then $\operatorname{Sg}^{\mathbf{A}}(X) = \bigcup_{n \in \omega} X_n$.

- Clones

Theorem 2. *Let A be a set and F a set of operations on A. Define*

$$F_0 = \operatorname{Proj}(A);$$
$$F_{n+1} = F_n \cup \{ f[g_1, \ldots, g_k] : f \in F,\ k = \operatorname{rank} f \text{ and } g_1, \ldots, g_k \in F_n \cap \operatorname{Op}_m(A), \text{ some } m \in \omega \}, \quad \text{for } n \in \omega.$$

Then $\operatorname{Clo}^A(F) = \bigcup_n F_n$.

- Terms

Definition 3. Let $\rho \colon \mathcal{F} \to \omega$ be a similarity type and X a set disjoint from $\mathcal{F}$. We define, by recursion on n, the sets T_n of words on $X \cup \mathcal{F}$ by

$$T_0 = \{ \langle w \rangle : w \in X \cup \mathcal{F}_0 \};$$
$$T_{n+1} = T_n \cup \{ f s_1 s_2 \ldots s_k : f \in \mathcal{F},\ k = \rho(f) \text{ and } s_1, \ldots, s_k \in T_n \}.$$

Finally, we define $T_\rho(X) = \bigcup_{n \in \omega} T_n$, called the set of *terms of type ρ over X*.

A possible type for terms

```
inductive term : Type
  | Var : term
  | nary : n : nat → g : term^n → term
```

```
inductive term : nat → Type
  | Var 0 : term
  | nary n : term^n → term
```

Example $f : term^n \to term$

$g_i : term^m \to term \qquad i \in \{1, \ldots, n\}$

$f[g_1, \ldots, g_n] : term^m \to term$

(what if the g_i have different arities?)

The Term Algebra
or Clone of term operations

Definition 4. For every basic n-ary operation symbol f of type ρ let $f^{\mathbf{T}_\rho(X)}$ be the n-ary operation on $T_\rho(X)$ that maps an n-tuple $(t_1, \ldots, t_n)$ to the term $ft_1 \ldots t_n$. We define $\mathbf{T}_\rho(X)$ to be the algebra with universe $T_\rho(X)$ and with basic operations $f^{\mathbf{T}_\rho(X)}$ for $f \in \mathcal{F}$.

A Typical Theorem/Proof: The term algebra is "absolutely free" or "initial"

Theorem 4.21. *Let ρ be a similarity type.*

(1) $\mathbf{T}_\rho(X)$ *is generated by* X.

(2) *For every algebra* $\mathbf{A}$ *of type* ρ *and every function* $h\colon X \to A$ *there is a unique homomorphism* $\bar{h}\colon \mathbf{T}_\rho(X) \to \mathbf{A}$ *such that* $\bar{h}\restriction_X = h$.

Proof. The definition of $T_\rho(X)$ exactly parallels the construction in Theorem 1. That accounts for (1). For (2), we define $\bar{h}(t)$ by induction on $|t|$. Suppose $|t| = 0$. Then $t \in X \cup \mathcal{F}_0$. If $t \in X$ then define $\bar{h}(t) = h(t)$. For $t \in \mathcal{F}_0$, $\bar{h}(t) = t^{\mathbf{A}}$. Note that since $\mathbf{A}$ is an algebra of type ρ and t is a nullary operation symbol, $t^{\mathbf{A}}$ is defined.

For the inductive step, let $|t| = n + 1$. Then $t = f(s_1, \ldots, s_k)$ for some $f \in \mathcal{F}_k$ and $s_1, \ldots, s_k$ each of height at most n. We define

$$\bar{h}(t) = f^{\mathbf{A}}\big(\bar{h}(s_1), \ldots, \bar{h}(s_k)\big).$$

By its very definition, $\bar{h}$ is a homomorphism.

Finally, the uniqueness of $\bar{h}$ . . . □

The End

Thank you!