More Work for Robin: Universal Algebra in Everyday Programming Logic, and Concomitant Challenges for Restriction Categories

Ernie Manes
University of Massachusetts at Amherst

June 9, 2012

1 Talk Objectives

Robin and I advertised a *Boolean restriction category* as an abstract category of partial functions which supports classical reasoning.

We'll look at three equivalent definitions of a BRC.

But wait! Does everyday programming logic support classical reasoning?

In everyday programming logic, “and” is not commutative.

var x : string;
if (Length(x)>0) and (x[1]='A') then . . .
if (x[1]='A') and (Length(x)>0) then . . .

are different.

We'll consider $if_p(f, g)$ for

Case I: p is total ($p \in$ Boolean algebra)

Case II: p can diverge, $if_p(f, g)$ computable if f, g are, ($p \in$?)

Case III: p can diverge, possess oracle for halting problem ($p \in$??)

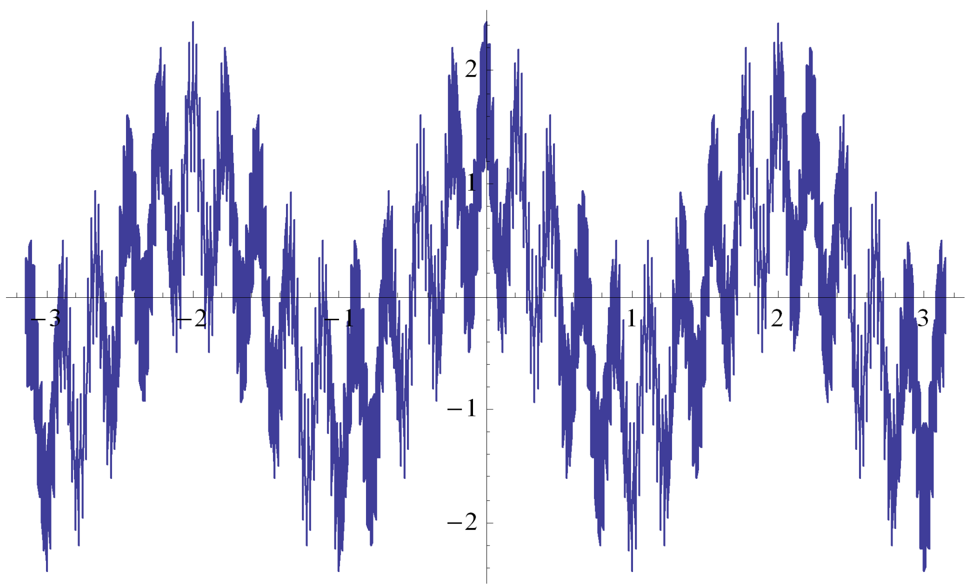
The univeral-algebraic results we discuss invite further work in restriction categories.

So let's get going.

But wait! What order do we compose in?

Can we figure this out from context?

$$\begin{aligned} \overline{g\,\overline{f}} &= \overline{g}\,\overline{f} \\ \overline{g}\,f &= \overline{gf} \end{aligned}$$


2
1
−1
−2
−3
−2
−1
1
2
3

2 Boolean Restriction Categories

A **restriction category** (Cockett and Lack, 2002) is a category $\mathcal{X}$ equipped with a unary operation $X \xrightarrow{f} Y \quad \mapsto$ $X \xrightarrow{\overline{f}} X$ satisfying the four axioms

(R.1) $f\,\overline{f} = f$

(R.2) $Y \xleftarrow{f} X \xrightarrow{g} Z, \quad \overline{f}\,\overline{g} = \overline{g}\,\overline{f}$

(R.3) $Y \xleftarrow{f} X \xrightarrow{g} Z, \quad \overline{g\,\overline{f}} = \overline{g}\,\overline{f}$

(R.4) Every $X \xrightarrow{f} Y$ is **deterministic** in that for all $Y \xrightarrow{g} Z$, $\overline{g}\,f = f\,\overline{gf}$

$\mathcal{X}(X,Y)$ is a poset under the **restriction ordering** $f \leq g$ if $g\,\overline{f} = f$. Composition on either side is monotone.

$R(X) = \{\overline{f} : X \xrightarrow{f} Y\} = \{X \xrightarrow{e} X : e = \overline{e}\}$ is the set of **restriction idempotents**, and it forms a meet semilattice under $\leq$ with $e \wedge f = ef = fe$.

In a restriction category, $f : X \to Y$ is **total** if $\overline{f} = id_X$. All monics are total.

If $\mathcal{X}$ is a **split** restriction category (in that all restriction idempotents split), let $\mathcal{M}$ be the class of all **restriction monics**, the monics that arise from such splittings.

Completeness Theorem (Cockett and Lack, 2002) A split restriction category is restriction isomorphic to the partial morphism category induced by the subcategory of total maps and $\mathcal{M}$-subobjects. The restriction is given by

$$\overline{[X \xleftarrow{m} A \xrightarrow{f} X]} \;=\; [X \xleftarrow{m} A \xrightarrow{m} X]$$

Thus a restriction category is a "category of partial maps", noting that the idempotent completion of a restriction category is a split restriction category.

Carboni, Lack and Walters 1993: An *extensive category* is one in which finite coproducts exist and are well-behaved (i.e., are like those of **Set**).

Manes 1992: (Standing on the shoulders of Elgot, Bloom and others): A *Boolean category* is a category suitable for (possibly non-deterministic) computation in which finite coproducts exist and are well-behaved (i.e., are like those of **Set**).

How are these categories defined?

A **Boolean category** (a) has finite coproducts, (b) is such that coproduct injections pull back along any morphism to coproduct injections, (c) if $X \xrightarrow{f} X \xleftarrow{f} X$ is a coproduct, $X = 0$, subject to

(B) Coproduct injections pull back coproducts

If (B) is strengthened to

(E) all morphisms pull back coproducts

we get an **extensive category**.

Example Rel, sets and relations, is Boolean and plays the metamathematical role for Boolean categories that **Ab** does for abelian categories.

Note: **Rel** does not have all pullbacks.

Example Sets and bags forms a Boolean category.

When is a Boolean category extensive?

In any category with initial 0, say that $f : X \to Y$ is **null** if it factors $f = X \xrightarrow{g} 0 \to Y$.

Say that f is **total** if $W \xrightarrow{t} X \xrightarrow{f} Y$ null $\Rightarrow$ t null.

In a Boolean category, 0 is "strict" in that every total $X \to 0$ is an isomorphism.

In any category, say that $f : X \to Y$ is **deterministic** if for every coproduct $Q \leftarrow Y \to Q'$ there exists a commutative diagram

$$\begin{tikzcd}
P \arrow[r] \arrow[d] & X \arrow[d, "f"] & P' \arrow[l] \arrow[d] \\
Q \arrow[r] & Y & Q' \arrow[l]
\end{tikzcd}$$

with the top row a coproduct.

Theorem (Manes 1992, Corollary 12.3) A category is extensive if and only if it is a Boolean category in which all morphisms are total and deterministic.

Toward Boolean restriction categories.

In a Boolean category:

Coproduct injections are monic. A **summand** is a subobject represented by a coproduct injection.

The poset $Summ(X)$ of all summands of X is always a Boolean algebra.

For $P, Q \in Summ(X)$, $P \to P \cup Q \leftarrow Q$ is a coproduct if and only if $P \cap Q = 0$.

For $f : X \to Y$, the pullback

$$\begin{tikzcd} Ker(f) \arrow[r] \arrow[d] & 0 \arrow[d] \\ X \arrow[r, "f"'] & Y \end{tikzcd}$$

Defines the **kernel** $Ker(f)$ of f. The complementary summand to $Ker(f) \in Summ(X)$ is the **domain** $Dom(f)$ of f.

A **Boolean restriction category** is a Boolean category with 0 a zero object such that for $f : X \to Y$,

$$\begin{tikzcd}
Dom(f) \arrow[r, "i"] \arrow[dr, "i"'] & X \arrow[d, "\overline{f}"] & Ker(f) \arrow[l] \arrow[dl, "0"] \\
& X &
\end{tikzcd}$$

defines a restriction.

Note that, unlike restriction categories and allegories which are categories with additional structure, a category is or is not a Boolean restriction category.

When is a Boolean category a BRC?

Theorem (Manes 2006) For $\mathcal{X}$ a Boolean category with zero object,

$\mathcal{X}$ is a Boolean restriction category $\Leftrightarrow$ every morphism is deterministic

When is a category a BRC?

Theorem A category is a Boolean restriction category if and only if it is the partial morphism category $Par(\mathcal{X}, \mathcal{M})$ with $\mathcal{X}$ an extensive category and $\mathcal{M}$ its coproduct injections.

Moreover, if the extensive category $\mathcal{X}$ has a terminal object 1 then the monad $X + 1$ classifies these partial morphisms.

Example: The partial morphism category of any Boolean topos.

When is a restriction category a BRC?

Theorem (Cockett and Manes, 2009). A restriction category is a BRC if and only if

- it has finite coproducts.
- the initial object is a zero.
- restriction idempotent split and the split monics involved are coproduct injections.
- Given $f, g : X \to Y$ with $f\,\overline{g} = g\,\overline{f}$ then with respect to the restriction ordering $f \leq g \Leftrightarrow g\,\overline{f} = f$, $f \vee g$ exists and composition on either side preserves such suprema.

Here goes a segue.

Where such a supremum arises is in

$$\text{if } \overline{p} \text{ then } f \text{ else } g \;=\; f\overline{p} \vee g\overline{p}'$$

A theme of this talk is: let such supremum be everywhere-defined, to allow a universal-algebraic description.

3 Any coproduct gives an if-then-else

Let $P \xrightarrow{i} X \xleftarrow{j} Q$ a coproduct in any category $\mathcal{X}$.

Define a binary operation $fg = if_{PQ}(f, g)$ on $\mathcal{X}(X, Y)$ by

$$\begin{tikzcd}
P \arrow[r, "i"] \arrow[d, "i"'] & X \arrow[d, "fg"] & Q \arrow[l, "j"'] \arrow[d, "j"] \\
X \arrow[r, "f"'] & Y & X \arrow[l, "g"]
\end{tikzcd}$$

In a Boolean restriction category, $Q = P'$ and $fg = f\overline{p} \vee g\overline{p}'$.

Proposition In any category, fg is a rectangular band.

Proof $ff \; i = f \; i$, $ff \; j = f \; j$ so $ff = f$. Similarly, $(fg)h = fh = f(gh)$. $\square$

Continue with $P \xrightarrow{i} X \xleftarrow{j} Q$

For $f, g : X \to Y$, one checks

$$f \,\mathcal{L}\, g \;\Leftrightarrow f\ j = g\ j$$
$$f \,\mathcal{R}\, g \;\Leftrightarrow f\ i = g\ i$$

Thus the semigroup isomorphism

$$\mathcal{X}(X,Y) \to \mathcal{X}(X,Y)/\mathcal{L} \;\times\; \mathcal{X}(X,Y)/\mathcal{R}$$

maps f to its restrictions to P and Q.

For a converse, see Exercise 3.

A network is the sum of its paths.

For example, one conceptualizes the following formal sum:

$$\begin{aligned} if_p(f, if_q(g,h)) &= fp + (gq + hq')p' \\ &= fp + gqp' + hq'p' \end{aligned}$$

With this end, let $\mathcal{X}$ now be semiadditive. Thus it has a zero object 0 and a coproduct $X \xrightarrow{in_1} X + X \xleftarrow{in_2} X$ is also a product

$$X \xleftarrow{\begin{pmatrix}1\\0\end{pmatrix}} X + X \xrightarrow{\begin{pmatrix}0\\1\end{pmatrix}} X$$

$\mathcal{X}(X,Y)$ is an abelian monoid via

$$f + g \quad = \quad X \xrightarrow{\begin{pmatrix}1 & 1\end{pmatrix}} X + X \xrightarrow{\begin{pmatrix}f\\g\end{pmatrix}} Y$$

Relative to the coproduct $P \xrightarrow{i} X \xleftarrow{j} Q$, define corresponding guards $p, q : X \to X$ by

$$\begin{aligned} p &= X \xrightarrow{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} P \xrightarrow{i} X \\ q &= X \xrightarrow{\begin{pmatrix} 0 \\ 1 \end{pmatrix}} Q \xrightarrow{j} X \end{aligned}$$

By construction, these are split idempotents whose monics are coproduct injections. Moreover, $pq = qp = 0$, $p + q = 1$.

It follows at once that for

$$\begin{tikzcd} P \arrow[r, "i"] \arrow[d, "i"'] & X \arrow[d, "fg"] & Q \arrow[l, "j"'] \arrow[d, "j"] \\ X \arrow[r, "f"'] & Y & X \arrow[l, "g"] \end{tikzcd}$$

$fg = fp + gq$.

4 Universal Algebra

Operations and equations, e.g. semigroups, groups, lattices, rings, modules over a rig, but not fields.

A quotient algebra of A is A/R where the equivalence relation R is a **congruence**, that is, is also a subalgebra of $A \times A$.

For a subclass $\mathcal{A}$, $P\mathcal{A}$, $S\mathcal{A}$, $Q\mathcal{A}$ is the class of all products, subalgebras, quotient algebras of algebras in $\mathcal{A}$.

$\mathcal{A}$ is a **variety** if it is closed under P, S and Q. Denote the smallest variety containing $\mathcal{A}$ by $Var(\mathcal{A})$.

Note: The concepts generalize to categories. For example, restriction categories and allegories are varieties of categories!

Surprising Examples

Huntington 1933: $(B, \vee, (\cdot)')$ is a Boolean algebra (for unique $0, 1$) if and only if

$$\begin{aligned} x \vee y &= y \vee x \\ x \vee (y \vee z) &= (x \vee y) \vee z \\ (x' \vee y)' \vee (x' \vee y')' &= x \end{aligned}$$

Sholander 1951: $(L, \vee, \wedge)$ is a distributive lattice if and only if

$$\begin{aligned} x \vee (x \wedge y) &= x \\ x \vee (y \wedge z) &= (z \vee x) \wedge (z \vee x) \end{aligned}$$

Theorem (Garrett Birkhoff, 1935)

- $\mathcal{A}$ is a variety if and only if it is the class of all algebra satisfying a set of further equations in the same operations.
- $Var(\mathcal{A}) = QSP(\mathcal{A})$.
- The equations satisfied by all algebras in $Var(\mathcal{A})$ are precisely those equations satisfied by all algebras in $\mathcal{A}$.
- Every variety has free algebras.
- Any variety is generated by its free algebra on ω generators. (This requires that operations are finitary, which we assume).

Example (Tarski, 1946) Let A be the free group on 2 generators. Then $Var(A)$ is all groups because the free group on ω generators is a subgroup of A.

5 Subdirect Irreducibility

If $0 \neq p \neq 1$ in a Boolean algebra B, $B \to [0,p] \times [0,p']$, $q \mapsto (p \wedge q, p' \wedge q)$ is a Boolean algebra isomorphism.

Corollary A finite Boolean algebra has 2^n elements where n is the number of atoms.

Garrett Birkhoff 1935 generalized product decompositions. A **subdirect embedding** of algebra A in a family $\mathcal{B}$ of algebras is a subalgebra $A \to \Pi B_i$ with all $B_i \in \mathcal{B}$ and all $A \to \Pi B_i \xrightarrow{pr_j} B_j$ surjective.

A is **subdirectly irreducible** if $|A| > 1$ and A admits no non-trivial dubdirect embedding, i.e. if $A \to \Pi B_i$ is subdirect, some $A \to \Pi B_i \xrightarrow{pr_j} B_j$ is an isomorphism.

Birkhoff proved:

Proposition For $|A| > 1$, A is subdirectly irreducible if and only if the intersection of all non-diagonal congruences on A is again non-diagonal.

Proof idea If $\mathcal{R}$ is the set of all non-diagonal congruences, consider the canonical map $A \to \prod_{R \in \mathcal{R}} A/R$.

Corollary Every simple algebra is subdirectly irreducible.

Corollary Every two-element algebra is simple, hence subdirectly irreducible.

Birkhoff then proved:

Theorem Let A be a (finitary!) algebra with $|A| > 1$. Then A admits a subdirect embedding $A \to \Pi\, B_i$ with each B_i subdirectly irreducible.

Proof idea By Zorn's Lemma, given $x \neq y$ let R_{xy} be a maximal congruence not containing (x, y). The canonical map $A \to \Pi_{x \neq y} A/R_{xy}$ is the desired subdirect embedding.

Corollary (Stone 1936) Every Boolean algebra is isomorphic to a Boolean algebra of sets.

Proof 2 is the only subdirect irreducible.

Corollary 2 generates the variety of Boolean algebras. This means truth tables can be used to establish any Boolean equation.

Example

Let $(G, +, 0)$ be an abelian group and also a meet semilattice $(G, \wedge)$. Consider the axioms

(BR) $x \wedge (y + z) = (x \wedge y) + (x \wedge z)$

(LOG) $x + (y \wedge z) = (x + y) \wedge (x + z)$

With (BR) get Boolean rings with 2 as unique subdirect irreducible.

With (LOG) get abelian lattice-ordered groups with every subgroup of $\mathbb{R}$ being subdirect irreducible.

6 The Lattice of Congruences

For any {finitary} algebra A, its congruences form a complete {algebraic} lattice $Cong(A)$.

Say that $R, S \in Cong(A)$ **permute** if $RS = SR$. In that case, $RS = R \vee S = SR$.

Theorem (Mal'cev 1954) In a variety of algebras, congruences permute if and only if there exists a ternary term $\tau(x, y, z)$ with

$$\tau(x, x, y) = y, \quad \tau(x, y, y) = x$$

In general, if congruences permute then $Cong(A)$ is a modular lattice.

Example For groups, $\tau(x, y, z) = xy^{-1}z$ is a Mal'cev term. This shows

- $HK = KH$ for K, H normal subgroups.
- Normal subgroups form a modular lattice.

Theorem (Alden Pixley 1963) In a variety of algebras, congruences permute and all lattices $Cong(A)$ are distributive if and only if there exists a "two-thirds minority" term $p(x, y, z)$ with

$$p(x, y, x) = p(x, y, y) = p(y, y, x) = x$$

Example Heyting algebras have a two-thirds minority term and hence so does Boolean algebras. For Boolean algebras, a suitable example is

$$p(x, y, z) \ = \ (x \wedge z) \vee (x \wedge y' \wedge z') \vee (x' \wedge y' \wedge z)$$

Thus the congruences of a Boolean algebra satisfy

$$\begin{aligned} R \cap (ST) \ &= \ (R \cap S)(R \cap T) \\ R(S \cap T) \ &= \ RS \cap RT \end{aligned}$$

7 Primal Algebras

Let F_X be the free algebra generated by X. Elements are equivalence classes of terms under the equations. For example, the free semigroup is all non-empty lists $x_1 \cdots x_n$ with $n > 0$. For example, xyz is the equivalence class $[x(yz)] = [(xy)z]$. Finding canonical forms such as "$[a(b(cd))]$" is the **word problem**.

The **interpretation** of an n-variable term τ in an algebra A is the function $A^n \to A$ obtained as the image of $[\tau]$ under the unique homomorphism $\psi_n : F_n \to A^{A^n}$ which maps $i \in n$ to the ith projection.

Algebra A is **primal** if A is finite with at least two elements and is such that ψ_n is surjective for all $n > 0$ –every function interprets some term.

If P is primal and A is an algebra in $Var(P)$, congruences on A permute and A has a distributive congruence lattice. This is immediate from Pixley's theorem.

Example In the variety of Boolean algebras, 2 is primal. Sierpinski's proof of this will emerge later.

In the exercises you will prove: every primal algebra is simple and has no proper subalgebras.

Algebra A is **equationally complete** if $Var(A)$ has no proper subvarieties.

Theorem (Rosenbloom, 1942) A primal algebra is equationally complete.

Theorem (Krauss, 1942) Let P be a primal algebra.

- Each finite algebra in $Var(P)$ is isomorphic to P^m for some m.
- P is the only primal algebra in $Var(P)$. For example, the Boolean algebra $4 = \{0, 1, x, x'\}$ is not primal because any $f : 4 \to 4$ such that $f(0) = x$ is not a Boolean term.
- Two varieties each generated by a primal algebra of the same cardinality are isomorphic.

For example, if one knows that $\mathbb{Z}_2$ is a primal generator of the variety of rings with unit with $x^2 = x$ (which is true), then a Boolean algebra is the same thing as a ring with unit with $x^2 = x$.

Proposition For primal P and $n \geq 0$ an integer, the free algebra generated by n in $Var(P)$ is P^{P^n}.

Proof $\psi_n : F_n \to P^{P^n}$ is surjective by primal and injective since F_n and P satisfy the same equations.

Theorem (Tah-Kai Hu, 1969) If P is primal, $Var(P)$ is equivalent to the category of Boolean algebras.

Proof Idea For A an algebra in $Var(P)$, the set ΨA of homomorphisms $A \to P$ is closed in the compact space P^A induced by the discrete topology on finite P, and so is a Stone space. Then $\Psi : Var(P)^{op} \to$ Stone spaces is an equivalence of categories.

8 McCarthy's Equations for if-then-else

We now enter Case II, letting tests diverge and giving up $if_p(f, f) = f$ and $p \wedge q = q \wedge p$. We have these universal-algebraic questions:

- What is the theory of $if_p(f, g)$?
- What sort of an algebra M do $p, q, ...$ range over?
- How does such M act on an abelian monoid?

We let $p \wedge q$, $p \vee q$ take their usual "short-circuit evaluation" meaning in computer programming.

John McCarthy 1963

$$\begin{aligned}
if_1(f,g) &= f \\
if_0(f,g) &= g \\
if_p(if_p(f,g),h) &= if_p(f,h) \quad = \quad if_p(f, if_p(g,h)) \\
if_{(p\wedge q)\vee(p'\wedge r)}(f,g) &= if_p(if_q(f,g), if_r(f,g)) \\
if_p(if_q(f,g), if_q(t,u)) &= if_q(if_p(f,t), if_p(g,u)) \\
if_p(if_q(f,g),h) &= if_p(if_q(if_p(f,f), if_p(g,g)), h) \\
if_p(f, if_q(g,h)) &= if_p(f, if_q(if_p(g,g), if_p(h,h)))
\end{aligned}$$

Completeness theorem These equations reduce each term to a canonical form and distinct canonical forms differ in the standard model.

Thus $fg = p(f,g)$ is a semigroup satisfying the **law of the redundant middle** $fgh = fh$ (third equation above). This is not a rectangular band because $ff \neq f$.

9 McCarthy Algebras

What do $p, q, ...$ range over? Boole introduced the "Boolean" connectives, but these were not axiomatized until Huntington 1904. Similarly, McCarthy used the short-circuit connectives, but these were not axiomatized until the paper of Fernando Guzmán and Craig Squier in 1990. They called these algebras "C-algebras" after "Conditional logic". By analogy to the situation with Boole, we feel these should be called McCarthy algebras.

A **McCarthy algebra** is $(M, \vee, \wedge, (\cdot)', 0, 2)$ subject to

(M.1) $x'' = x$

(M.2) $(x \wedge y)' = x' \vee y'$

(M.3) $(x \wedge y) \wedge z = x \wedge (y \wedge z)$

(M.4) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

(M.5) $(x \vee y) \wedge z = (x \wedge z) \vee (x' \wedge y \wedge z)$

(M.6) $x \vee (x \wedge y) = x$

(M.7) $(x \wedge y) \vee (y \wedge x) = (y \wedge x) \vee (x \wedge y)$

(M.8) $0 \wedge x = 0,\ 2 \wedge x = 2$

(M.9) $2' = 2,\ 0' \wedge 2 = 2$

Some "Boolean" properties hold: Here, $1 = 0'$.

$$\begin{aligned} x \wedge x &= x \\ x \wedge y &= x \wedge (x' \vee y) \\ x \vee (x' \wedge x) &= x \\ (x \vee x') \wedge y &= (x \wedge y) \vee (x' \wedge y) \\ (x \vee x') \wedge x &= x \\ x \wedge 1 &= x \quad = \quad 1 \wedge x \end{aligned}$$

These properties fail in every nontrivial McCarthy algebra:

$$\begin{aligned} x \wedge x' &= 0 \\ x \vee x' &= 1 \end{aligned}$$

$3 = \{0, 1, 2\}$ is a McCarthy algebra.

x	x'
0	1
1	0
2	2

$x \wedge y$	0	1	2
0	0	0	0
1	0	1	2
2	2	2	2

$x \vee y$	0	1	2
0	0	1	2
1	1	1	1
2	2	2	2

3 is simple, hence subdirectly irreducible.

Theorem (Guzmán and Squier) 3 is the only subdirectly irreducible McCarthy algebra.

Corollary Every McCarthy algebra is a subalgebra of 3^I.

Corollary All potential McCarthy algebra equations can be verified or disproved by 3-truth tables. The Guzmán-Squier equations are complete!

Corollary In a McCarthy algebra, $x = x' \Rightarrow x = 2$. Thus every finite McCarthy algebra has an odd number of elements.

Proof Obvious in 3^I.

Corollary In a McCarthy algebra, define

$$if_p(q, r) \quad = \quad (p \wedge q) \vee (p' \wedge r)$$

Then all of McCarthy's equations hold.

Implementation of if-then-else in a BRC

The next idea was employed by Guzmán and Squier and was due originally to Alfred Foster, 1951 who was investigating certain rings.

Let B be a Boolean algebra. Let M_B be the set of all pairs (p, q) with $p, q \in B$, $p \wedge q = 0$. Define

$$\begin{aligned} 0 &= (0, 1) \\ 2 &= (0, 0) \\ (p, q)' &= (q, p) \\ (p, q) \wedge (r, s) &= (p \wedge q, q \vee (p \wedge s)) \\ (p, q) \vee (r, s) &= (p \vee (q \wedge r), q \wedge s) \end{aligned}$$

Then M_B is a McCarthy algebra.

We can do this in any Boolean restriction category.

The origin of the idea is simple. There is a natural bijection between 3^I and pairs of disjoint subsets of I via

$$I \xrightarrow{f} 3 \quad \mapsto \quad (f^{-1}0, f^{-1}1)$$

The formulas above are the transport of the pointwise operations in 3^I.

This leads us to

Proposition For every odd $n \geq 3$ there exists an n-element McCarthy algebra.

Proof Given a McCarthy algebra M, consider it a subalgebra of some 3^I using the pairs-of-sets representation. If $I \subset J$ with J strictly larger, the new 0 and 1 are the pairs $(0, J)$, $(J, 1)$ which together with the old pairs constitute a new McCarthy algebra with two more elements.

Corollary 3 is not a primal McCarthy algebra.

Proof Otherwise, every finite McCarthy algebra would have 3^m elements.

10 An Oracle for Halting

What would it take to make 3 primal?

Let $u_{xyz} : 3 \to 3$ be $0 \mapsto x$, $1 \mapsto y$, $2 \mapsto z$.

Define $if : 3^3 \to 3$ by $if_p(q, r) = (p \wedge q) \vee (p' \wedge r)$.

Now observe for any $f : 3^4 \to 3$ that

$$\begin{aligned} f(w, x, y, z) \;=\; & if_{u_{100}z}(f(w, x, y, 0), \\ & \quad if_{u_{001}z}(f(w, x, y, 2), f(w, x, y, 1))) \end{aligned}$$

This works the same way for any $n > 0$, not just $n = 4$. For example,

$$Halt \;=\; u_{110} \;=\; \lambda_z\, if_{u_{100}z}(0, if_{u_{001}z}(2, 1))$$

This 3 is primal providing if and the two unary operations u_{100}, u_{001} interpret terms. This idea dates fo Sierpinski, 1945: "If X is finite, any function $X^n \to X$ is a composition of binary functions".

Now $if : 3^3 \rightarrow 3$ already interprets a McCarthy term, so we need only to get u_{100}, $u_{001} : 3 \rightarrow 3$.

Write u_{010} as $p^{\downarrow}$. Then

$$\begin{aligned} Halt(p) &= u_{110} \quad = \quad (p \vee 1)^{\downarrow} \\ u_{100} &= p'^{\downarrow} \\ u_{001} &= (p \vee 1)^{\downarrow\prime} \end{aligned}$$

Throwing in $p^{\downarrow}$ provides an oracle for the halting problem because

$$Halt(p) \;=\; p'^{\downarrow} \vee (p \vee 1)^{\downarrow} \quad = \quad u_{100} \vee u'_{001}$$

In that case, 3 is primal.

A **McCarthy algebra with halt** or Mh**-algebra** adds to McCarthy algebra a unary operation $p^{\downarrow}$ with equations

$$
\begin{aligned}
0^{\downarrow} &= 0 = 2^{\downarrow}, \quad 1^{\downarrow} = 1 \\
p \wedge q^{\downarrow} &= p \wedge (p \wedge q)^{\downarrow} \\
p^{\downarrow} \vee p^{\downarrow\prime} &= 1 \\
p &= p^{\downarrow} \vee p
\end{aligned}
$$

We immediately have:

3 is a primal Mh-algebra.

Also, by exactly the Guzmán-Squier proof, 3 is the only subdirectly irreducible Mh-algebra.

Thus every Mh-algebra embeds in some power 3^I, and $Var(3)$ is all Mh-algebras.

By Hu's theorem, Mh-algebras is equivalent to Boolean algebras.

A more direct proof of this "Morita equivalence" is given in Manes 1993:

- For H an Mh-algebra, $H_{\#} = \{a \in H : a^{\downarrow} = a\}$ is closed under $\{0, 1, (\cdot)', \vee, \wedge\}$ and is a Boolean algebra under these operations.
- $H \mapsto H_{\#}$ is an equivalence of categories.
- The inverse equivalence maps B to the McCarthy algebra $M_B = \{(p, q) \in B^2 : p \wedge q = 0\}$ which is an Mh-algebra if $(p, q)^{\downarrow} = (p, p')$.

Thus every Mh-algebra has form M_B. General implementation of the short-circuit operations can be done in a Boolean restriction category!

Boolean algebras are rings. What a about Mh-algebras?

For prime p, a p**-ring** is a commutative ring satisfying $px = 0$, $x^p = x$. The concept is due to McCoy and Montgomery, 1937.

Take note of this equation $x^p = x$ with regard to later remarks about abelian restriction semigroups.

In 1957, Alfred Foster proved that $\mathbb{Z}_p$ is a primal p-ring which generates the variety of all p-rings. We conclude from Krauss' theorem:

Theorem Mh-algebras $\cong$ 3-rings as a variety.

11 A Cayley theorem for McCarthy algebras

An idea championed by Steve Bloom

For X a set, define nullary 1, unary f' and binary $f \wedge g$ on the set $[X^2 \to X]$ of binary operations on X by

$$\begin{aligned} 1(x,y) &= x \\ f'(x,y) &= f(y,x) \\ (f \wedge g)(x,y) &= f(g(x,y),y) \end{aligned}$$

We say two binary operations $f, g : X^2 \to X$ **commute** if each is a homomorphism in the other.

Theorem (Bloom, Ésik and Manes 1990)

1. Let $\mathcal{A} \subset [X^2 \to X]$ consist of rectangular bands any two of which commute, and be closed under 1, f' and $f \wedge g$. Then $\mathcal{A}$ is a Boolean algebra.
2. If B is a Boolean algebra then $B \to [B^2 \to B]$, $p \mapsto px \vee p'y$, is an injective Boolean algebra homomorphism.

Consider

$p \vee q$	0	1	2
0	0	1	2
1	1	1	1
2	2	2	2

$p\|q$	0	1	2
0	0	1	2
1	1	1	2
2	2	2	2

$$p \| q \quad = \quad (p \wedge (q \vee q')) \vee (p' \wedge q)$$

Both of these are **regular extensions of 2-valued logic** in the sense of Kleene 1952.

Cayley theorem For a McCarthy algebra, $M \to [M^2 \to M]$,

$$p \ \mapsto \ I_p(q, r) = (p \wedge q) \, \| \, (p' \wedge r)$$

is an injective homomorphism in 0, $(\cdot)'$, $\wedge$.

12 Abelian Restriction Semigroups

Proposition (James Johnson and Ernie Manes, 1970). Let $\mathcal{V}$ be a variety of abelian monoids equipped with additional unary operations, each of which is a monoid endomorphism together with any set of further equations. Then there exists a rig R with $\mathcal{V} \cong R\text{-}Mod$.

Corollary Abelian restriction semigroups arise as the modules over a rig.

Abelian restriction semigroups are abelian semigroups together with $\overline{x}$ such that

$$\begin{aligned} x\,\overline{x} &= x \\ \overline{\overline{x}} &= \overline{x} \\ \overline{xy} &= \overline{x}\,\overline{y} \end{aligned}$$

By the way: A question from the cited paper which I believe remains open is to characterize those rigs R for which R-Mod is balanced.

Observation Let A be a commutative semigroup such that $\forall\, x\ \exists\, n > 1\ x^n = x$. Then A is an inverse semigroup, hence a restriction semigroup; $\overline{x} = x^{n-1}$.

- Every idempotent is a restriction idempotent.
- $x \leq y \;\Leftrightarrow\; x^2 = xy$.
- Total $\Leftrightarrow$ invertible.

As a special case, let $A = \prod F_i$ be a product of (the multiplicative semigroups of) finite fields with $\bigvee |F_i| < \infty$. Then

- if $x \perp y$ (that is, $\overline{x}\,\overline{y} = 0$), $x \vee y$ exists and is $x + y$.
- A is a locally Boolean poset in the restriction order.

Many examples of abelian restriction semigroups exist besides these:

- Any abelian monoid with trivial restriction.
- The lower sets of an abelian restriction monoid forms an abelian restriction monoid under the setwise operations IJ, $\overline{I}$.
- One can take arbitrary products, subalgebras and quotients.

Open Question What is the rig whose modules are all abelian restriction monoids?

13 Conclusion

So, where are the promised challenges for restriction categories?

By now you're all brain dead.

So I wrote them all down on the handout!

CONGRATS ON SURVIVING TUTORIAL 20!