Everything is Relative – Some Remembrances of Pieter Hofstra's Personality and Work

Jaap van Oosten

Department of Mathematics
Utrecht University

October Fest, Ottawa, October 29, 2022

Partial Combinatory Algebras (PCAs)

A *Partial Combinatory Algebra* is a set A together with a partial map $A \times A \rightharpoonup A$ (the *application map*). Also here we write, for elements $a, b \in A$, $ab\downarrow$ to indicate that the pair (a, b) is in the domain of the application map.

Moreover, a PCA A should have elements k and s satisfying:

$$\begin{gathered} \mathsf{k}x\downarrow \\ (\mathsf{k}a)b = a \\ (\mathsf{s}a)b\downarrow \end{gathered}$$

and: if $(ac)(bc)\downarrow$ then $((\mathsf{s}a)b)c\downarrow$ and

$$((\mathsf{s}a)b)c = (ac)(bc)$$

.

PCAs are building blocks of toposes. For each PCA A we have a category $\mathrm{Asm}(A)$ of *assemblies* on A:
An assembly over A is a pair (X, E) where X is a set and $E(x)$ is a *nonempty* subset of A, for each $x \in X$.
A *morphism of assemblies* $(X, E) \to (Y, F)$ is a function $f : X \to Y$ of sets, for which there is an element $a \in A$ such that for all $x \in X$ and all $b \in E(x)$, $ab \in F(f(x))$. One says that a *tracks* the function f.

The category Asm(A) is locally cartesian closed, regular, has a weak subobject classifier (is a quasi-topos). Moreover, Asm(A) comes with an adjunction

$$(\Gamma : \mathsf{Ass}(A) \to \mathrm{Set}) \dashv (\nabla : \mathrm{Set} \to \mathsf{Ass}(A))$$

$\Gamma(X, E) = X$; $\nabla(X) = (X, \lambda x.A)$.
The category Asm(A) also has a *natural numbers object*.

Theorem (Pitts 1980; Carboni, Freyd, Scedrov 1988): the exact completion of $\mathsf{Asm}(A)$, $\mathsf{Asm}(A)_{\mathrm{ex/reg}}$, is a topos, the *realizability topos* over A.

We now wish to understand: how functorial is the construction $A \mapsto \mathrm{RT}(A)$?

It turns out that there is a very nice categorical structure on the class of PCAs, which was first explored by John Longley in his thesis (1995).

Let A, B be PCAs. An *applicative morphism* $A \to B$ is a total relation γ (we think of γ as a function from A to the set of nonempty subsets of B, so (A, γ) is an assembly over B) for which there is an element $\mathrm{r} \in B$ which satisfies:

For each pair a, a' of elements of A and $b \in \gamma(a), b' \in \gamma(a')$, if $aa' \downarrow$ in A then $\mathrm{r}bb' \downarrow$ in B, and $\mathrm{r}bb' \in \gamma(aa')$.

The element r *realizes* the morphism γ. Composition of morphisms is composition of total relations.

We think of γ as a *simulation* in B of computations in A; the element r is a machine that translates code for an A-program into code for a B-program.

Theorem (Longley 1995): every applicative morphism $A \stackrel{\gamma}{\to} B$ gives rise to a regular functor $\mathsf{Asm}(\gamma) : \mathsf{Asm}(A) \to \mathsf{Asm}(B)$ which makes the diagram

$$\begin{array}{ccc} \mathsf{Asm}(A) & \xrightarrow{\mathsf{Asm}(\gamma)} & \mathsf{Asm}(B) \\ & \underset{\Gamma}{\searrow} & \downarrow \Gamma \\ & & \mathrm{Set} \end{array}$$

commute. Conversely, every regular functor making this diagram commute, is of the form $\mathsf{Ass}(\gamma)$ for an essentially unique applicative morphism $\gamma : A \to B$.
In fact the functor $\mathrm{Asm} : \mathsf{PCA} \to \mathsf{REG}/\mathrm{Set}$, which sends an assembly A to the functor $\Gamma_A : \mathrm{Asm}(A) \to \mathrm{Set}$, is locally an equivalence.

I. Computationally dense morphisms

What do geometric morphisms between realizability toposes look like?

Fundamental observation by Peter Johnstone (2013): Every geometric morphism $\mathrm{RT}(A) \to \mathrm{RT}(B)$ restricts to an adjunction between the categories of assemblies.

The left adjoint of such a restriction is always a regular functor commuting with the Γ's, and therefore corresponds to an applicative morphism $B \stackrel{\gamma}{\to} A$. The question then is:

For which applicative morphisms $\gamma : B \to A$ does the regular functor $\mathrm{Ass}(\gamma) : \mathrm{Ass}(B) \to \mathrm{Ass}(A)$ have a right adjoint?

A generalization: ordered PCAs.

An ordered PCA (OPCA) is a poset $(A, \leq)$ with a partial application function $a, b \mapsto ab$ for which the following hold:

- the domain of the application function is downwards closed and application is order-preserving on its domain;
- there exist k and s in A such that $\mathsf{k}ab \leq a$ and $\mathsf{s}abc \preceq ac(bc)$ (i.e., if $ac(bc)\downarrow$ then $\mathsf{s}abc\downarrow$ and $\mathsf{s}(abc) \leq ac(bc)$).

Main example: given an ordinary PCA A, its powerset $\mathcal{P}(A)$ becomes an OPCA if we put: $\alpha\beta\downarrow$ iff for all $a \in \alpha, b \in \beta$, $ab\downarrow$, in which case we let $\alpha\beta$ be the subset $\{ab \mid a \in \alpha, b \in \beta\}$.

An applicative morphism between OPCAs A and B is a function $f : A \to B$ for which there is some $r \in B$ satisfying: whenever $aa'{\downarrow}$ in A, then $rf(a)f(a'){\downarrow}$ in B, and $rf(a)f(a') \leq f(aa')$.
An assembly over an OPCA A is a pair (X, E) with X a set and $E(x)$ a *nonempty* downwards closed subset of A, for each $x \in X$.
Similarly to Longley's treatment we have a local equivalence $\mathrm{Asm} : \mathsf{OPCA} \to \mathsf{REG}/\mathrm{Set}$. Also, Pitts' theorem generalizes: $\mathrm{Asm}(A)$ is a regular category, and $\mathrm{Asm}(A)_{\mathrm{ex/reg}}$ is a realizability topos $\mathsf{RT}(A)$.
We are interested in applicative morphisms $f : B \to A$ for which $\mathrm{Asm}(f) : \mathrm{Asm}(B) \to \mathrm{Asm}(A)$ has a right adjoint. Because then, applying the exact completion we obtain a geometric morphism of realizability toposes.

Call an applicative morphism $f : B \to A$ between OPCAs *computationally dense* if for all $a \in A$ there exists $b \in B$ such that whenever $af(c)\downarrow$ for $c \in B$, we have $bc\downarrow$ in B, and $f(bc) \leq af(c)$.
It says: every endomap on B which is realized (modulo f) in A, is already (up to order) realized in B.
Theorem (Hofstra 2003): $\mathrm{Asm}(f) : \mathrm{Asm}(B) \to \mathrm{Asm}(A)$ has a right adjoint if and only if f is computationally dense.

A further generalization: relative OPCAs.
If A is an OPCA, a *filter* on A is a subset F which:

- is upwards closed
- is closed under the application map
- contains elements k and s which satisfy the axioms for A being an OPCA.

We call the pair (A, F) a *relative PCA*.
For example: let $B = \mathbb{N}^{\mathbb{N}}$, $A = \mathcal{P}(B)$. We could take F the set of those elements of A which contain at least one computable function (Kleene-Vesley 1965).
An assembly over a relative PCA (A, F) is just an assembly over A, but a morphism of such assemblies has to be tracked by an element of F. Again, $\mathrm{Asm}(A, F)_{\mathrm{ex/reg}}$ is a topos, $\mathrm{RT}(A, F)$.
It turns out that for important closure properties of realizability toposes one has to move to these relative realizability toposes (Zoethout 2022)

II. BCOs and triposes

In a very nice paper (Hofstra 2006), Pieter analyzed the notion of a relative OPCA from a more primitive notion. The central definition is that of a *basic combinatorial object* (BCO).

Definition: a BCO is a poset $(\Sigma, \leq)$ together with a set F_Σ of partial endofunctions on Σ, which satisfies the following axioms:

1. Every function in F_Σ has downwards closed domain and is order-preserving on its domain;
2. there is a total function $i \in F_\Sigma$ such that $i(a) \leq a$ for all $a \in \Sigma$ (i is a "weak identity");
3. For each pair $f, g \in F_\Sigma$ there is $h \in F_\Sigma$ satisfying: $\mathrm{domain}(gf) \subseteq \mathrm{domain}(h)$ and $h(a) \leq g(f(a))$ for $a \in \mathrm{domain}(gf)$ (we have some sort of "weak composition").

Note that every poset is a BCO, as is every monoid, every partial combinatory algebra. More importantly, every relative OPCA is a BCO in a natural way.

A morphism between BCOs $(\Sigma, \leq, F_\Sigma) \to (\Theta, \leq, F_\Theta)$ is a function $\phi : \Sigma \to \Theta$ satisfying:

1. there exists $u \in F_\Theta$ such that for each inequality $a \leq a'$ in Σ we have $u(\phi(a)) \leq \phi(a')$ in Θ ("ϕ is order-preserving modulo u");
2. for all $f \in F_\Sigma$ there is $g \in F_\Theta$ with $g(\phi(a)) \leq \phi(f(a))$ ("g simulates the functional behaviour of f relative to ϕ").

The category BCO is order-enriched and has a monad on it, the Downset monad $\mathcal{D}$, which is Kock-Zöberlein (algebras are left adjoint to units).

Moreover, for every BCO Σ we have a Set-indexed preorder $[-,\Sigma]$: $[X,\Sigma]$ is the set of functions from X to Σ, and for $\phi,\psi \in [X,\Sigma]$ we have $\phi \leq \psi$ if and only if there is some $f \in F_\Sigma$ such that $f(\phi(x)) \leq \psi(x)$ for all $x \in X$.

We shall be interested in the question: when is $[-,\Sigma]$ a tripos?

Theorem (Hofstra 2006): Let Σ be a BCO, and $[-, \Sigma]$ its associated Set-indexed preorder. Then the following two statements are equivalent:

1. Σ is an OPCA with filter Φ, so the preorder on $[X, \Sigma]$ is given by: $\alpha \leq \beta$ iff there is $a \in \Phi$ such that for all $x \in X$ and $b \in \alpha(x)$, $ab \in \beta(x)$.
2. $[-, \mathcal{D}\Sigma]$ is a tripos.

A refinement: a *pre-implicative* OPCA is a filtered OPCA A together with suitable maps $\bigwedge : \mathcal{P}(A) \to A$ and $\Rightarrow: A \times A \to A$.
Theorem (vO–Zou 2016): $[-, \Sigma]$ is a tripos if and only if Σ is a pre-implicative OPCA.

III. Dialectica Monads.

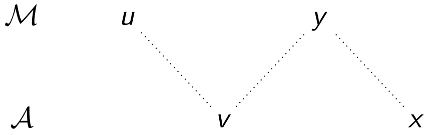
In 1958, Gödel published a paper about which he had been mulling since the early 1940's: *On a hitherto unused extension of the finitary point of view*, in which he sought to reduce the consistency of Peano Arithmetic to that of the theory of quantifier-free equations involving primitive recursive functionals of finite type. In 2002, Martin Hyland (following De Paiva's Ph.D. thesis) gave a categorical construction of this interpretation. Suppose we have a posetal fibration $p : \mathbb{P} \to \mathbb{T}$, where $\mathbb{T}$ is a category with finite products. We construct a new category $\mathrm{Dial}(p)$:

- objects are triples (U, X, α) with $U, X \in \mathbb{T}$ and $\alpha \in p^{U \times X}$;
- maps $(U, X, \alpha) \to (V, Y, \beta)$ are pairs $f : U \to V, F : U \times Y \to X$ of morphisms in $\mathbb{T}$ such that for the morphisms

$$\begin{aligned} \langle \pi_0, F \rangle : &\quad U \times Y \to U \times X \\ \langle f\pi_0, \pi_1 \rangle : &\quad U \times Y \to V \times Y \end{aligned}$$

  we have $\langle \pi_0, F \rangle^*(\alpha) \le \langle f\pi_0, \pi_1 \rangle^*(\beta)$ in $p^{U \times Y}$

A simple interpretation. Let us think of a fibration of sets. Consider the following two-move game, between Merlin (evil) and Arthur (the good guy). Merlin starts by picking $u \in U$, Arthur responds by picking $v \in V$. Merlin now picks $y \in Y$, and Arthur picks $x \in X$. End of the game:



Now we have special subsets $\alpha \subseteq U \times X$, $\beta \subseteq V \times Y$, and the stipulation is that Arthur wins if $(v, y) \in \beta$ whenever $(u, x) \in \alpha$. Note that Arthur's choice of x may depend on both Merlin's moves u and y. Hence a *strategy* for Arthur consists of a pair of functions $(f : U \to V, F : U \times Y \to X)$, and if this satisfies $(f(u), y) \in \beta$ whenever $(u, F(u, y) \in \alpha$ for all u, y, then (f, F) is a *winning strategy*.

Now suppose that α and β are the complements of graphs of functions A, B respectively. Then taking the contrapositive of the winning condition, we see that (f, F) is a winning strategy if $F(u, y) = A(u)$ whenever $y = B(f(u))$, that is: *the pair* (f, F) *determines a one-query oracle computation of* A *with oracle* B.

This game can be analyzed further: for a function A we have the one-move game G_A: $\mathcal{M}$erlin picks some ξ, $\mathcal{A}$rthur responds with σ, and wins if $A(\xi) = \sigma$. The "oracle game" above is now a cut-off version of the "implication game" $G_B \Rightarrow G_A$ (in the sense of Hyland-Ong).

Pieter set out to analyse the Hyland-De Paiva Dialectica construction as a composition of canonical constructions on fibrations.
Let $p : E \to B$ be a fibration; we assume B has finite products.
Say *p has simple coproducts* if for every projection $I \times J \xrightarrow{\pi} I$ in B, the functor $\pi^* : p^I \to p^{I \times J}$ has a left adjoint, and these left adjoints satisfy the Beck-Chevalley condition.
Similarly, one defines *simple products*. Let p^{op} be the opposite fibration (i.e. the fibration over B such that $(p^{\mathrm{op}})^I = (p^I)^{\mathrm{op}}$): then p has simple products if and only if p^{op} has simple coproducts.

To any fibration $p : E \to B$ one can add simple coproducts in a universal way: let

$$\begin{array}{ccc} \mathrm{Fam}(E) & \longrightarrow & E \\ \downarrow & & \downarrow{\scriptstyle p} \\ B^{\to} & \xrightarrow[\mathrm{dom}]{} & B \end{array}$$

be a pullback. Let $\mathrm{Fam}(p)$ be the composition

$$\mathrm{Fam}(E) \longrightarrow B^{\to} \xrightarrow{\mathrm{cod}} B$$

$\mathrm{Fam}(p)$ is the free fibration on p with coproducts; it has a subfibration $\mathrm{Sum}(p)$ which is universal (w.r.t. p) with simple coproducts.
Similarly, we have $\mathrm{Prod}(p) = \mathrm{Sum}(p^{\mathrm{op}})^{\mathrm{op}}$.
We have: the operations Sum and Prod have the structure of pseudo-monads on Fib(p), the category of fibrations on p.
Moreover, there is an appropriate distributive law between them, guaranteeing that also the composition $\mathrm{Sum}{\circ}\mathrm{Prod}$ has a pseudo-monad structure.

Lemma: there is a natural isomorphism of fibrations

$$\mathrm{Dial}(p) \simeq \mathrm{Sum}(\mathrm{Prod}(p))$$

Theorem: Assume B is cartesian closed. Then the pseudo-algebras for the pseudomodad Dial on $\mathrm{Fib}(B)$ are the fibrations with simple products and coproducts satisfying the distributivity

$$\forall u \exists x \alpha(i, u, x) \simeq \exists f \forall u \alpha(i, fu, u)$$

Pieter Hofstra was my first PhD student, but also a friend. I recall with gratitude his hospitality in 2006 when I stayed with him and Miyoung in Calgary, and had an unforgettable ride in the Rocky Mountains.

I was also deeply moved when he organized (together with Benno van den Berg, who was a PhD student of Moerdijk roughly the same time as Pieter was working with me) a special PSSL celebrating my and Thomas Streicher's 60th birthdays, in 2018.

His death is still unthinkable.

Literature:

A. Carboni, P. Freyd, A. Scedrov, A Categorical Approach to Realizability and Polymorphic Types, MFPS, LNCS 298, 1988.

K. Gödel, Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes, Dialectica 12, 1958.

P. Hofstra, J. van Oosten, Ordered partial combinatory algebras, Math.Proc.Cam.Phil.Soc.134, 2003.

P. Hofstra, All realizability is relative, Math.Proc.Cam.Phil.Soc. 141, 2006.

P. Hofstra, The dialectica monad and its cousins, CRM Proceedings & Lecture Notes 53, 2011.

J.M.E. Hyland, Proof Theory in the Abstract, APAL 114, 2002.

J.M.E. Hyland, C.-H. L. Ong, On Full Abstraction for PCF: I, II and III, Information and Computation 163, 2000

P.T. Johnstone, Geometric Morphisms of Realizability Toposes, TAC 28(9), 2013.

S.C.Kleene, R.E. Vesley, The Foundations of Intuitionistic Mathematics, North-Holland 1965.
J. Longley, Realizability Toposes and Language Semantics, PhD thesis, Edinburgh, 1995.
J. van Oosten, T. Zou, Classical and Relative realizability, TAC 31(22), 2016.
Valeria de Paiva, The Dialectica Categories, PhD thesis, Cambridge 1990.
A.M. Pitts, The Theory of Triposes, PhD thesis, Cambridge 1980.
J. Zoethout, Computability Models and Realizability Toposes, PhD thesis, Utrecht 2022.