

Category-Partial Orders and Proof Principles

Ralf Hinze

Computing Laboratory, University of Oxford
Wolfson Building, Parks Road, Oxford, OX1 3QD, England
ralf.hinze@comlab.ox.ac.uk
<http://www.comlab.ox.ac.uk/ralf.hinze/>

June 2008

```
data List = [] | Nat : List
```

```
append :: (List, List) → List
```

```
append ([], bs) = bs
```

```
append (a : as, bs) = a : append (as, bs)
```

$$\forall x : \text{List} . P(x)$$
$$P(x) \iff \text{append}(x, []) = x$$

Case $P([])$:

$$\begin{aligned} & \text{append}([], []) \\ = & \quad \{ \text{definition of append} \} \\ & [] \end{aligned}$$

Case $P(a : as)$:

$$\begin{aligned} & \text{append}(a : as, []) \\ = & \quad \{ \text{definition of append} \} \\ & a : \text{append}(as, []) \\ = & \quad \{ \text{ex hypothesi} \} \\ & a : as \end{aligned}$$

$\text{append} :: (\text{List}, \text{List}) \rightarrow \text{List}$
 $\text{append } (\text{as}, \text{bs}) = \text{foldr } (:) \text{ bs as}$

$$\begin{aligned} & \text{append (as, [])} \\ = & \quad \{ \text{definition of append} \} \\ & \text{foldr (:) [] as} \\ = & \quad \{ \text{reflection: foldr (:) [] = id} \} \\ & \text{as} \end{aligned}$$

Cat + \subseteq ?

Ordering objects

A *category-partial order* is a pair $\langle \mathbb{C}, \sqsubseteq \rangle$ where

- ▶ \mathbb{C} is a category and
- ▶ \sqsubseteq is a subcategory of \mathbb{C} that is a partial order on the objects of \mathbb{C} .

Ordering morphisms

Let $f : A \rightarrow B$ and $g : C \rightarrow D$, then

$$f \sqsubseteq g$$

iff $A \sqsubseteq C$, $B \sqsubseteq D$ and the following diagram commutes.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \parallel & & \parallel \\ C & \xrightarrow{g} & D \end{array} \iff \sqsubseteq_{B,D} \cdot f = g \cdot \sqsubseteq_{A,C}$$

Properties

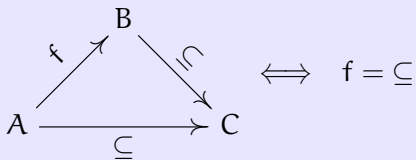
- ▶ \sqsubseteq on morphisms is a partial order.
- ▶ Let $f, g : A \rightarrow B$, then

$$f \sqsubseteq g \quad \iff \quad f = g$$

Examples

- ▶ $\langle \mathbf{Set}, \subseteq \rangle$: $f \sqsubseteq g$ iff f is the restriction of g to A .
- ▶ Functor categories: $\mathbb{D}^{\mathbb{C}}$ is a c-po if \mathbb{D} is one.

In Set:



Split transitivity

Let $f : A \rightarrow B$, then

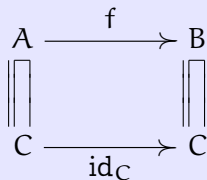
$$\sqsubseteq_{B,C} \cdot f = \sqsubseteq_{A,C} \iff f = \sqsubseteq_{A,B}$$

A c-po that satisfies this property is called a *split c-po*.

An equivalent formulation

Let $f : A \rightarrow B$, then

$$f \sqsubseteq \text{id}_C \quad \Longrightarrow \quad f = \sqsubseteq_{A,B}$$



In **Set** the inclusion morphisms are monos.

$$\subseteq \cdot f_1 = \subseteq \cdot f_2 \quad \iff \quad f_1 = f_2$$

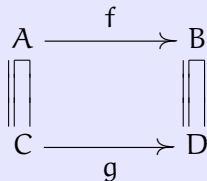
Monic c-pos

A c-po is called a *monic c-po* if the arrows $\sqsubseteq_{A,B}$ are monos:
Let $f_1, f_2 : A \rightarrow B$ in \mathbb{C} , then

$$\sqsubseteq_{B,C} \cdot f_1 = \sqsubseteq_{B,C} \cdot f_2 \quad \iff \quad f_1 = f_2$$

Properties

In a monic c-po the lower arrow uniquely determines the upper arrow.

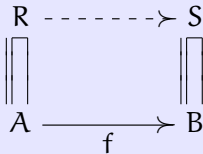


Contracts

Let $f : A \rightarrow B$, then

$$f \in R \rightarrow S \quad :\iff \quad \exists g : R \rightarrow S . g \sqsubseteq f$$

Think of $R \rightarrow S$ as a *contract* with *precondition* R and *postcondition* S . But note that the postcondition can't be weaker than B .



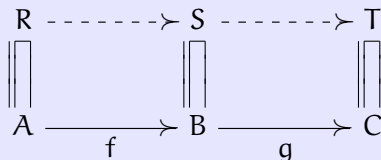
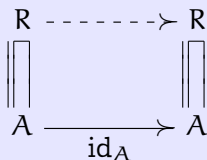
An aside: The category of contracts

- Identity:

$$R \sqsubseteq A \iff \text{id}_A \in R \rightarrow R$$

- Composition: Let $f : A \rightarrow B$ and $g : B \rightarrow C$, then

$$f \in R \rightarrow S \wedge g \in S \rightarrow T \implies g \cdot f \in R \rightarrow T$$



Initial objects

$$0 \dashrightarrow^{\text{id}_A} A$$

Universal property

$$i_A = h \iff h : 0 \rightarrow A$$

Reflection

Set $A = 0$ and $h = \text{id}_0$.

We obtain

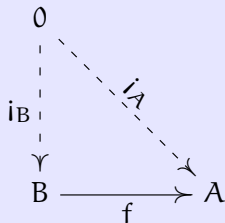
$$i_0 = \text{id}_0$$

Fusion

Let $f : B \rightarrow A$ and set $h = f \cdot i_B : 0 \rightarrow A$.

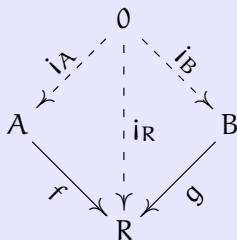
We obtain

$$i_A = f \cdot i_B \iff f : B \rightarrow A$$



The mother of all proof principles

$$\frac{f : A \rightarrow R \quad g : B \rightarrow R}{f \cdot i_A = g \cdot i_B}$$



A special case: Set $B = R$ and $g = \text{id}_R$.

We obtain

$$\frac{f : A \rightarrow R}{f \cdot i_A = i_R}$$

So, the proof principle implies fusion.

A more special case: Set $f = \sqsubseteq_{A,R}$.

We obtain

$$\frac{A \sqsubseteq R}{i_A \sqsubseteq i_R}$$

$$\frac{A \sqsubseteq R}{i_R \in 0 \rightarrow A}$$

$$\begin{array}{ccc}
 0 & \overset{i_A}{\dashrightarrow} & A \\
 \parallel & & \parallel \\
 0 & \underset{i_R}{\dashrightarrow} & R
 \end{array}$$

An even more special case: Set $R = 0$.

We obtain

$$\frac{A \sqsubseteq 0}{i_A \sqsubseteq i_0}$$

$$\frac{A \sqsubseteq 0}{i_0 \in 0 \rightarrow A}$$

Recall that $i_0 = \text{id}_0$. So, in a split c-po this implies:

$$\frac{A \sqsubseteq 0}{A = 0}$$

An even more special case: Set $R = 0$.

We obtain

$$\frac{A \sqsubseteq 0}{i_A \sqsubseteq i_0} \qquad \frac{A \sqsubseteq 0}{i_0 \in 0 \rightarrow A}$$

Recall that $i_0 = \text{id}_0$. So, in a split c-po this implies:

$$\frac{A \sqsubseteq 0}{A = 0}$$

Cospans

Given: objects A and B .

A cospan is an object C with two morphisms $f : A \rightarrow C$ and $g : B \rightarrow C$.

$$A \xrightarrow{f} C \xleftarrow{g} B$$

The category of cospans

Cospans are the objects of the category $\mathbf{Cospan}(A, B)$.
Morphisms in $\mathbf{Cospan}(A, B)$ are morphisms in the
underlying category that make the following diagram
commute.

$$\begin{array}{ccccc} A & \xrightarrow{f} & C & \xleftarrow{g} & B \\ \text{id}_A \downarrow & & \downarrow h & & \downarrow \text{id}_B \\ A & \xrightarrow{f'} & C' & \xleftarrow{g'} & B \end{array}$$

Coproducts

The initial object in $\mathbf{Cospan}(A, B)$ is the coproduct of A and B .

Notation:

$$\begin{array}{ccccc} A & \xrightarrow{\text{inl}} & A + B & \xleftarrow{\text{inr}} & B \\ \text{id}_A \downarrow & & \vdots & & \downarrow \text{id}_B \\ A & \xrightarrow{f} & C & \xleftarrow{g} & B \end{array}$$

Ordering cospans

$$\langle C, f, g \rangle \sqsubseteq \langle C', f', g' \rangle \quad :\iff \quad C \sqsubseteq C' \wedge f \sqsubseteq f' \wedge g \sqsubseteq g'$$

Proof principle: case analysis

$$\frac{R \sqsubseteq C}{i_C \in 0 \rightarrow R}$$

$$\frac{R \sqsubseteq C \quad f \in A \rightarrow R \quad g \in B \rightarrow R}{f \nabla g \in A + B \rightarrow R}$$

A special case: $C = 0$.

$$\frac{\frac{R \sqsubseteq 0}{R = 0} \quad R \sqsubseteq A + B \quad \text{inl} \in A \rightarrow R \quad \text{inr} \in B \rightarrow R}{R = A + B}$$

F-algebras

Given: a functor $F : \mathbb{C} \rightarrow \mathbb{C}$.

An F-algebra is an object T with a morphism $f : FT \rightarrow T$.

$$FT \xrightarrow{f} T$$

The category of F-algebras

F-algebras are the objects of the category $\mathbf{Alg}(F)$.
Morphisms in $\mathbf{Alg}(F)$ are morphisms in the underlying
category that make the following diagram commute.

$$\begin{array}{ccc} FT & \xrightarrow{f} & T \\ \text{Fh} \downarrow & & \downarrow h \\ FT' & \xrightarrow{f'} & T' \end{array}$$

Initial algebras

The initial object in $\mathbf{Alg}(F)$ is the least fixed point of F .

Notation:

$$\begin{array}{ccc} F(\mu T) & \xrightarrow{\text{in}} & \mu T \\ \downarrow F(f) & & \downarrow (f) \\ FT & \xrightarrow{f} & T \end{array}$$

Ordering F-algebras

$$\langle T, f \rangle \sqsubseteq \langle T', f' \rangle \quad :\Leftrightarrow \quad T \sqsubseteq T' \wedge f \sqsubseteq f'$$

Proof principle: induction

$$\frac{R \sqsubseteq C}{i_C \in 0 \rightarrow R}$$

$$\frac{R \sqsubseteq C \quad f \in FR \rightarrow R}{(f) \in \mu F \rightarrow R}$$

A special case: $C = 0$.

$$\frac{R \sqsubseteq 0}{R = 0}$$

$$\frac{R \sqsubseteq \mu F \quad \text{in} \in FR \rightarrow R}{R = \mu F}$$

`data` Base A = 1 + Nat × A

`type` List = μBase

$P = \{x : \text{List} \mid \text{append}(x, []) = x\}$

$$\frac{\text{nil} \in 1 \rightarrow P \quad \text{cons} \in \text{Nat} \times P \rightarrow P}{\text{nil} \nabla \text{cons} \in \text{Base } P \rightarrow P}$$
$$\frac{\text{in} \in \text{Base } P \rightarrow P}{P = \text{List}}$$

Correctness of insertion sort

$$\text{Ord} = \{x : \text{List} \mid \text{ordered } x\}$$

$$\frac{\text{nil} \in 1 \rightarrow \text{Ord} \quad \text{insert} \in \text{Nat} \times \text{Ord} \rightarrow \text{Ord}}{\frac{\text{nil} \nabla \text{insert} \in \text{Base Ord} \rightarrow \text{Ord}}{(\text{nil} \nabla \text{insert}) \in \text{List} \rightarrow \text{Ord}}}$$

Epilogue

- ▶ Simple and general framework for studying proof principles.
- ▶ Nicely links proof principles to contracts.
- ▶ The development dualises: proof principles for terminal objects (products, final coalgebras).
- ▶ *But*, the requirements also dualise: epic inclusion, cosplit transitivity which doesn't hold in Set .

