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

Prologue
Category-partial orders
Split c-pos
Monic c-pos
Initial objects
Proof principles
Coproducts
Initial algebras
Examples
Epilogue

$$\mathbf{data}\ \mathrm{List} = [\,] \mid \mathrm{Nat} : \mathrm{List}$$

$$\begin{aligned}
&\mathrm{append} :: (\mathrm{List},\ \mathrm{List}) \to \mathrm{List}\\
&\mathrm{append}\ \ ([\,],\quad \mathrm{bs}) \quad = \mathrm{bs}\\
&\mathrm{append}\ \ (\mathrm{a} : \mathrm{as}, \mathrm{bs}) \quad = \mathrm{a} : \mathrm{append}\ (\mathrm{as}, \mathrm{bs})
\end{aligned}$$

$$\forall x : \mathrm{List}\ .\ P(x)$$

$$P(x) \iff \mathrm{append}\ (x, [\,]) = x$$

Case $P([\,])$:

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

Case $P(a : as)$:

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

$$
\begin{aligned}
&\mathrm{append} :: (\mathrm{List}, \mathrm{List}) \to \mathrm{List}\\
&\mathrm{append}\ \ (as,\ \ bs) \ \ = \mathrm{foldr}\ (:)\ bs\ as
\end{aligned}
$$

Prologue
Category-partial orders
Split c-pos
Monic c-pos
Initial objects
Proof principles
Coproducts
Initial algebras
Examples
Epilogue

Prologue
Category-partial orders
Split c-pos
Monic c-pos
Initial objects
Proof principles
Coproducts
Initial algebras
Examples
Epilogue

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

$$\mathbf{Cat} + \subseteq \ ?$$

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

$$f \sqsubseteq g$$

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

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\sqsubseteq"'] & B \arrow[d, "\sqsubseteq"] \\ C \arrow[r, "g"'] & D \end{tikzcd} \iff \sqsubseteq_{B,D} \cdot f = g \cdot \sqsubseteq_{A,C}$$

Properties

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

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

Prologue

Category-partial orders

Split c-pos

Monic c-pos

Initial objects

Proof principles

Coproducts

Initial algebras

Examples

Epilogue

Prologue

Category-partial orders

Split c-pos

Monic c-pos

Initial objects

Proof principles

Coproducts

Initial algebras

Examples

Epilogue

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**:

$$\begin{tikzcd} & B \arrow[dr, "\subseteq"] & \\ A \arrow[ur, "f"] \arrow[rr, "\subseteq"'] & & C \end{tikzcd} \iff f = \subseteq$$

Split transitivity

Let $f : A \to B$, then

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

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

An equivalent formulation

Let $f : A \to B$, then

$$f \sqsubseteq id_C \qquad \Longrightarrow \qquad f = \sqsubseteq_{A,B}$$

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, phantom, sloped, "\sqsubseteq"] & B \arrow[d, phantom, sloped, "\sqsubseteq"] \\ C \arrow[r, "id_C"'] & C \end{tikzcd}$$

Prologue

Category-partial orders

Split c-pos

Monic c-pos

Initial objects

Proof principles

Coproducts

Initial algebras

Examples

Epilogue

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

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

Monic c-pos

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

$$\sqsubseteq_{B,C} \cdot f_1 = \sqsubseteq_{B,C} \cdot f_2 \qquad \Longleftrightarrow \qquad f_1 = f_2$$

Prologue

Category-partial orders

Split c-pos

Monic c-pos

Initial objects

Proof principles

Coproducts

Initial algebras

Examples

Epilogue

Properties

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

$$\begin{tikzcd}
A \arrow[r, tail, "f"] \arrow[d, phantom, sloped, "\sqsubseteq"] & B \arrow[d, phantom, sloped, "\sqsubseteq"] \\
C \arrow[r, tail, "g"'] & D
\end{tikzcd}$$

Contracts

Let $f : A \to B$, then

$$f \in R \to S \quad :\Longleftrightarrow \quad \exists g : R \to S \,.\, g \sqsubseteq f$$

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

$$\begin{tikzcd}
R \arrow[r, dashed, tail] \arrow[d, phantom, "\rotatebox{-90}{$\sqsubseteq$}"] & S \arrow[d, phantom, "\rotatebox{-90}{$\sqsubseteq$}"] \\
A \arrow[r, tail, "f"'] & B
\end{tikzcd}$$

Prologue
Category-partial orders
Split c-pos
Monic c-pos
Initial objects
Proof principles
Coproducts
Initial algebras
Examples
Epilogue

An aside: The category of contracts

- Identity:

$$R \sqsubseteq A \quad \iff \quad id_A \in R \to R$$

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

$$f \in R \to S \;\wedge\; g \in S \to T \quad \Longrightarrow \quad g \cdot f \in R \to T$$

$$\begin{tikzcd}
R \arrow[r, dashed, tail] \arrow[d, phantom, "\sqsubseteq" rotate=-90] & R \arrow[d, phantom, "\sqsubseteq" rotate=-90] \\
A \arrow[r, tail, "id_A"'] & A
\end{tikzcd}
\qquad
\begin{tikzcd}
R \arrow[r, dashed, tail] \arrow[d, phantom, "\sqsubseteq" rotate=-90] & S \arrow[r, dashed, tail] \arrow[d, phantom, "\sqsubseteq" rotate=-90] & T \arrow[d, phantom, "\sqsubseteq" rotate=-90] \\
A \arrow[r, tail, "f"'] & B \arrow[r, tail, "g"'] & C
\end{tikzcd}$$

Prologue

Category-partial orders

Split c-pos

Monic c-pos

Initial objects

Proof principles

Coproducts

Initial algebras

Examples

Epilogue

Initial objects

$$0 \xrightarrow{i_A} A$$

Universal property

$$i_A = h \quad \iff \quad h : 0 \to A$$

Reflection

Set $A = 0$ and $h = \mathrm{id}_0$.
We obtain

$$\mathsf{i}_0 \;=\; \mathrm{id}_0$$

Fusion

Let $f : B \to A$ and set $h = f \cdot i_B : 0 \to A$.
We obtain

$$i_A = f \cdot i_B \quad \Longleftarrow \quad f : B \to A$$

$$\begin{tikzcd}
0 \arrow[d, dashed, "i_B"'] \arrow[dr, dashed, "i_A"] & \\
B \arrow[r, "f"'] & A
\end{tikzcd}$$

Prologue
Category-partial orders
Split c-pos
Monic c-pos
Initial objects
Proof principles
Coproducts
Initial algebras
Examples
Epilogue

The mother of all proof principles

$$\frac{f : A \to R \qquad g : B \to R}{f \cdot i_A = g \cdot i_B}$$

$$\begin{tikzcd}
 & 0 \arrow[dl, dashed, "i_A"'] \arrow[dr, dashed, "i_B"] \arrow[dd, dashed, "i_R"] & \\
A \arrow[dr, "f"'] & & B \arrow[dl, "g"] \\
 & R &
\end{tikzcd}$$

Prologue

Category-partial orders

Split c-pos

Monic c-pos

Initial objects

Proof principles

Coproducts

Initial algebras

Examples

Epilogue

A special case: Set $B = R$ and $g = id_R$.
We obtain

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

So, the proof principle implies fusion.

Prologue

Category-partial orders

Split c-pos

Monic c-pos

Initial objects

Proof principles

Coproducts

Initial algebras

Examples

Epilogue

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

We obtain

$$\frac{A \sqsubseteq R}{i_A \sqsubseteq i_R} \qquad\qquad \frac{A \sqsubseteq R}{i_R \in 0 \to A}$$

$$\begin{tikzcd}
0 \arrow[r, dashed, tail, "i_A"] \arrow[d, equal] & A \arrow[d, "\sqsubseteq"] \\
0 \arrow[r, dashed, tail, "i_R"'] & R
\end{tikzcd}$$

Prologue
Category-partial orders
Split c-pos
Monic c-pos
Initial objects
Proof principles
Coproducts
Initial algebras
Examples
Epilogue

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

We obtain

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

Recall that $i_0 = id_0$. So, in a split c-po this implies:

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

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

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

Recall that $i_0 = id_0$. 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 $f : A \to C$ and $g : A \to C$.

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

Prologue
Category-partial orders
Split c-pos
Monic c-pos
Initial objects
Proof principles
Coproducts
Initial algebras
Examples
Epilogue

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.

$$
\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "id_A"'] & C \arrow[d, "h"] & B \arrow[l, "g"'] \arrow[d, "id_B"] \\
A \arrow[r, "f'"'] & C' & B \arrow[l, "g'"]
\end{tikzcd}
$$

Coproducts

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

Notation:

$$\begin{tikzcd}
A \arrow[r, "\mathit{inl}"] \arrow[d, "\mathit{id}_A"'] & A + B \arrow[d, dashed, "f \triangledown g"] & B \arrow[l, "\mathit{inr}"'] \arrow[d, "\mathit{id}_B"] \\
A \arrow[r, "f"'] & C & B \arrow[l, "g"]
\end{tikzcd}$$

Ordering cospans

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

Proof principle: case analysis

$$\frac{R \sqsubseteq C}{i_C \in 0 \to R} \qquad \frac{R \sqsubseteq C \qquad f \in A \to R \qquad g \in B \to R}{f \triangledown g \in A + B \to R}$$

Prologue

Category-partial orders

Split c-pos

Monic c-pos

Initial objects

Proof principles

Coproducts

Initial algebras

Examples

Epilogue

A special case: $C = 0$.

$$\frac{R \sqsubseteq 0}{R = 0} \qquad\qquad \frac{R \sqsubseteq A + B \qquad \mathit{inl} \in A \to R \qquad \mathit{inr} \in B \to R}{R = A + B}$$

F-algebras

Given: a functor $F : \mathbb{C} \to \mathbb{C}$.
An F-algebra is an object T with a morphism $f : FT \to T$.

$$FT \xrightarrow{\quad f \quad} T$$

The category of F-algebras

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

$$\begin{tikzcd}
\mathsf{F}\mathsf{T} \arrow[r, "f"] \arrow[d, "\mathsf{F}h"'] & \mathsf{T} \arrow[d, "h"] \\
\mathsf{F}\mathsf{T}' \arrow[r, "f'"'] & \mathsf{T}'
\end{tikzcd}$$

Prologue
Category-partial orders
Split c-pos
Monic c-pos
Initial objects
Proof principles
Coproducts
Initial algebras
Examples
Epilogue

Initial algebras

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

$$\begin{tikzcd}
\mathsf{F}(\mu\mathsf{T}) \arrow[r, "\mathsf{in}"] \arrow[d, "\mathsf{F}(\!|f|\!)"'] & \mu\mathsf{T} \arrow[d, dashed, "(\!|f|\!)"] \\
\mathsf{F}T \arrow[r, "f"'] & T
\end{tikzcd}$$

Prologue

Category-partial orders

Split c-pos

Monic c-pos

Initial objects

Proof principles

Coproducts

Initial algebras

Examples

Epilogue

Ordering F-algebras

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

Proof principle: induction

$$\frac{R \sqsubseteq C}{i_C \in 0 \to R} \qquad\qquad \frac{R \sqsubseteq C \qquad f \in FR \to R}{(\!|f|\!) \in \mu F \to R}$$

Prologue

Category-partial orders

Split c-pos

Monic c-pos

Initial objects

Proof principles

Coproducts

Initial algebras

Examples

Epilogue

A special case: $C = 0$.

$$\frac{R \sqsubseteq 0}{R = 0} \qquad\qquad \frac{R \sqsubseteq \mu F \qquad \mathit{in} \in F R \to R}{R = \mu F}$$

$$\mathbf{data}\ \mathrm{Base}\,A = 1 + \mathrm{Nat} \times A$$
$$\mathbf{type}\ \mathrm{List} = \mu\mathrm{Base}$$

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

$$\cfrac{\cfrac{\cfrac{\mathrm{nil} \in 1 \to P \qquad \mathrm{cons} \in \mathrm{Nat} \times P \to P}{\mathrm{nil} \mathbin{\triangledown} \mathrm{cons} \in \mathrm{Base}\,P \to P}}{\mathrm{in} \in \mathrm{Base}\,P \to P}}{P = \mathrm{List}}$$

Correctness of insertion sort

$$\mathrm{Ord} \quad = \quad \{\, x : \mathrm{List} \mid \mathrm{ordered}\; x \,\}$$

$$\frac{\dfrac{\mathrm{nil} \in 1 \to \mathrm{Ord} \qquad \mathrm{insert} \in \mathrm{Nat} \times \mathrm{Ord} \to \mathrm{Ord}}{\mathrm{nil} \mathbin{\triangledown} \mathrm{insert} \in \mathrm{Base}\,\mathrm{Ord} \to \mathrm{Ord}}}{(\!|\mathrm{nil} \mathbin{\triangledown} \mathrm{insert}|\!) \in \mathrm{List} \to \mathrm{Ord}}$$

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 $\mathbf{Set}$.

$$
\begin{tikzcd}
 & \{0\} \arrow[dr, "\{0 \mapsto 1\}"] & \\
\emptyset \arrow[ur, "\subseteq"] \arrow[rr, "\subseteq"'] & & \{1\}
\end{tikzcd}
$$