Breaking the Loop

Recursive Proofs for Coinductive Predicates

Henning Basold

CNRS, ENS Lyon

LIMD Seminar
Université Savoie, Bourget du Lac
14 June 2018

Original Motivation

- Syntactic logic for program equivalence in my thesis
- Recursive proof system based on later modality
- Recursion gives rise to proof search
- Many of the constructions are pedestrian
- Need for an abstract framework

Original Motivation

- Syntactic logic for program equivalence in my thesis
- Recursive proof system based on later modality
- Recursion gives rise to proof search
- Many of the constructions are pedestrian
- Need for an abstract framework

Motivation

Stream Differential Equations

Example (Constant Streams)

$$a^\omega : \mathbb{R}^\omega \qquad a^\omega_0 = a \qquad (a^\omega)' = a^\omega$$

Example (Point-wise Stream Addition)

$$\oplus : \mathbb{R}^\omega \to \mathbb{R}^\omega \to \mathbb{R}^\omega$$
$$(s \oplus t)_0 = s_0 + t_0$$
$$(s \oplus t)' = s' \oplus t'$$

Example (Stream of Positive Numbers)

$$s : \mathbb{R}^\omega \qquad s_0 = 1 \qquad s' = 1^\omega \oplus s$$

Point-wise Positive Streams

Example (Predicate Transformer)

$$\Phi(P \subseteq \mathbb{R}^\omega) = \{s \in \mathbb{R}^\omega \mid s_0 > 0 \land s' \in P\}$$

- Φ monotone
- Greatest fixed point $\nu\Phi$ exists
- $s \in \nu\Phi$ iff s is point-wise greater than 0

Positive Numbers are Greater Than 0

$$
\dfrac{
\textbf{(Next)}\;\dfrac{\text{(Def. of } s\text{)}\;\dfrac{\overline{\vdash 1 > 0}}{\vdash s_0 > 0}}{\vdash \blacktriangleright(s_0 > 0)}
\qquad
\dfrac{\dfrac{\dfrac{\dfrac{\overline{\blacktriangleright\varphi \vdash \blacktriangleright\varphi}}{\blacktriangleright\varphi \vdash \blacktriangleright(s \in \nu\Phi)}\;\textbf{(Pr)}}{\blacktriangleright\varphi \vdash \blacktriangleright(1^\omega \oplus s \in C(\nu\Phi))}\;\text{(Def. } C\text{)}}{\blacktriangleright\varphi \vdash \blacktriangleright(1^\omega \oplus s \in \nu\Phi)}\;\text{(}C\text{ compat.)}}{\blacktriangleright\varphi \vdash \blacktriangleright(s' \in \nu\Phi)}\;\text{(Def. of } s\text{)}
}{
\dfrac{\dfrac{\blacktriangleright\varphi \vdash \blacktriangleright(s_0 > 0 \land s' \in \nu\Phi)}{\blacktriangleright\varphi \vdash s \in \nu\Phi}\;\textbf{(Step)}}{\vdash s \in \nu\Phi}\;\textbf{(Löb)}
}\;\text{(}\blacktriangleright\text{ preserves } \land\text{)}
$$

Inference Rule

Positive Numbers are Greater Than 0

$$\dfrac{\dfrac{\dfrac{\textbf{(Next)}\;\dfrac{\text{(Def. of } s\text{)}\;\dfrac{\dfrac{}{\vdash 1 > 0}}{\vdash s_0 > 0}}{\vdash \blacktriangleright(s_0 > 0)} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\blacktriangleright\varphi \vdash \blacktriangleright\varphi}}{\blacktriangleright\varphi \vdash \blacktriangleright(s \in \nu\Phi)}\;\textbf{(Pr)}}{\blacktriangleright\varphi \vdash \blacktriangleright(1^\omega \oplus s \in C(\nu\Phi))}\;\text{(Def. } C\text{)}}{\blacktriangleright\varphi \vdash \blacktriangleright(1^\omega \oplus s \in \nu\Phi)}\;(C\text{ compat.})}{\blacktriangleright\varphi \vdash \blacktriangleright(s' \in \nu\Phi)}\;\text{(Def. of } s\text{)}}{\blacktriangleright\varphi \vdash \blacktriangleright(s_0 > 0 \wedge s' \in \nu\Phi)}\;(\blacktriangleright\text{ preserves }\wedge)}{{\color{red}\blacktriangleright\varphi} \vdash s \in \nu\Phi}\;\textbf{(Step)}}{\vdash s \in \nu\Phi}\;{\color{red}\textbf{(Löb)}}$$

Inference Rule

$$\varphi := s \in \nu\Phi$$

$$\dfrac{\Delta, \blacktriangleright\varphi \vdash \varphi}{\Delta \vdash \varphi}\;\textbf{(Löb)}$$

Positive Numbers are Greater Than 0

$$\dfrac{\dfrac{\dfrac{\textbf{(Next)}\;\dfrac{(\text{Def. of } s)\;\dfrac{\dfrac{}{\vdash 1 > 0}}{\vdash s_0 > 0}}{\vdash \blacktriangleright(s_0 > 0)} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\blacktriangleright \varphi \vdash \blacktriangleright \varphi}}{\blacktriangleright \varphi \vdash \blacktriangleright(s \in \nu\Phi)}\;\textbf{(Pr)}}{\blacktriangleright \varphi \vdash \blacktriangleright(1^\omega \oplus s \in C(\nu\Phi))}\;(\text{Def. } C)}{\blacktriangleright \varphi \vdash \blacktriangleright(1^\omega \oplus s \in \nu\Phi)}\;(C \text{ compat.})}{\blacktriangleright \varphi \vdash \blacktriangleright(s' \in \nu\Phi)}\;(\text{Def. of } s)}{\blacktriangleright \varphi \vdash {\color{red}\blacktriangleright(s_0 > 0 \land s' \in \nu\Phi)}}\;(\blacktriangleright \text{ preserves } \land)}{\blacktriangleright \varphi \vdash s \in \nu\Phi}\;{\color{red}\textbf{(Step)}}}{\vdash s \in \nu\Phi}\;\textbf{(Löb)}$$

Inference Rule

$$\begin{array}{c} \Delta \vdash \blacktriangleright(s \in \Phi(\nu\Phi)) \\ \hline\hline \Delta \vdash s \in \nu\Phi \end{array}\;\textbf{(Step)}$$

$$\Phi(P) = \{s \in \mathbb{R}^\omega \mid s_0 > 0 \land s' \in P\}$$

Positive Numbers are Greater Than 0

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash 1 > 0}}{\vdash s_0 > 0}\,\text{(Def. of } s\text{)}}{\vdash \blacktriangleright(s_0 > 0)}\,\textbf{(Next)} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\blacktriangleright \varphi \vdash \blacktriangleright \varphi}}{\blacktriangleright \varphi \vdash \blacktriangleright(s \in \nu\Phi)}\,\textbf{(Pr)}}{\blacktriangleright \varphi \vdash \blacktriangleright(1^\omega \oplus s \in C(\nu\Phi))}\,\text{(Def. } C\text{)}}{\blacktriangleright \varphi \vdash \blacktriangleright(1^\omega \oplus s \in \nu\Phi)}\,(C\text{ compat.})}{\blacktriangleright \varphi \vdash \blacktriangleright(s' \in \nu\Phi)}\,\text{(Def. of } s\text{)}}{\blacktriangleright \varphi \vdash \blacktriangleright(s_0 > 0 \wedge s' \in \nu\Phi)}\,(\blacktriangleright\text{ preserves } \wedge)}{\blacktriangleright \varphi \vdash s \in \nu\Phi}\,\textbf{(Step)}}{\vdash s \in \nu\Phi}\,\textbf{(Löb)}$$

Inference Rule

$$\dfrac{\Delta \vdash \blacktriangleright \varphi \wedge \blacktriangleright \psi}{\Delta \vdash \blacktriangleright(\varphi \wedge \psi)}\,(\blacktriangleright\text{ preserves } \wedge)$$

Positive Numbers are Greater Than 0

$$
\dfrac{
\dfrac{\dfrac{\dfrac{}{\vdash 1 > 0}}{\vdash s_0 > 0}\,\text{(Def. of } s\text{)}}{\vdash \blacktriangleright(s_0 > 0)}\,\textbf{(Next)}
\qquad
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\blacktriangleright \varphi \vdash \blacktriangleright \varphi}}{\blacktriangleright \varphi \vdash \blacktriangleright(s \in \nu\Phi)}\,\textbf{(Pr)}}{\blacktriangleright \varphi \vdash \blacktriangleright(1^\omega \oplus s \in C(\nu\Phi))}\,\text{(Def. } C\text{)}}{\blacktriangleright \varphi \vdash \blacktriangleright(1^\omega \oplus s \in \nu\Phi)}\,(C\text{ compat.})}{\blacktriangleright \varphi \vdash \blacktriangleright(s' \in \nu\Phi)}\,\text{(Def. of } s\text{)}
}{
\dfrac{\dfrac{\blacktriangleright \varphi \vdash \blacktriangleright(s_0 > 0 \wedge s' \in \nu\Phi)}{\blacktriangleright \varphi \vdash s \in \nu\Phi}\,\textbf{(Step)}}{\vdash s \in \nu\Phi}\,\textbf{(Löb)}
}\,(\blacktriangleright\text{ preserves } \wedge)
$$

Inference Rule

$$
\dfrac{\Delta \vdash \varphi}{\Delta \vdash \blacktriangleright \varphi}\,\textbf{(Next)}
$$

Positive Numbers are Greater Than 0

$$\dfrac{\dfrac{\dfrac{\textbf{(Next)}\;\dfrac{\text{(Def. of } s\text{)}\;\dfrac{\dfrac{}{\vdash 1 > 0}}{\vdash s_0 > 0}}{\vdash \blacktriangleright(s_0 > 0)} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\blacktriangleright\varphi \vdash \blacktriangleright\varphi}}{\blacktriangleright\varphi \vdash \blacktriangleright(s \in \nu\Phi)}\;\textbf{(Pr)}}{\blacktriangleright\varphi \vdash \blacktriangleright(1^\omega \oplus s \in C(\nu\Phi))}\;\text{(Def. } C\text{)}}{\blacktriangleright\varphi \vdash \blacktriangleright(1^\omega \oplus s \in \nu\Phi)}\;(C\text{ compat.})}{\blacktriangleright\varphi \vdash \blacktriangleright(s' \in \nu\Phi)}\;\text{(Def. of } s\text{)}}{\blacktriangleright\varphi \vdash \blacktriangleright(s_0 > 0 \wedge s' \in \nu\Phi)}\;(\blacktriangleright\text{ preserves } \wedge)}{\blacktriangleright\varphi \vdash s \in \nu\Phi}\;\textbf{(Step)}}{\vdash s \in \nu\Phi}\;\textbf{(Löb)}$$

Inference Rule

$$s : \mathbb{R}^\omega \qquad s_0 = 1 \qquad s' = 1^\omega \oplus s$$

Positive Numbers are Greater Than 0

$$\dfrac{\dfrac{\dfrac{\textbf{(Next)}\;\dfrac{\text{(Def. of }s\text{)}\;\dfrac{\overline{\vdash 1 > 0}}{\vdash s_0 > 0}}{\vdash \blacktriangleright(s_0 > 0)} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\overline{\blacktriangleright\varphi \vdash \blacktriangleright\varphi}}{\blacktriangleright\varphi \vdash \blacktriangleright(s\in\nu\Phi)}\;\textbf{(Pr)}}{\blacktriangleright\varphi\vdash\blacktriangleright(1^\omega\oplus s\in C(\nu\Phi))}\;\text{(Def. }C\text{)}}{\blacktriangleright\varphi\vdash\blacktriangleright(1^\omega\oplus s\in\nu\Phi)}\;(C\text{ compat.})}{\blacktriangleright\varphi\vdash\blacktriangleright(s'\in\nu\Phi)}\;\text{(Def. of }s\text{)}}{\blacktriangleright\varphi\vdash\blacktriangleright(s_0>0\wedge s'\in\nu\Phi)}\;(\blacktriangleright\text{ preserves }\wedge)}{\blacktriangleright\varphi\vdash s\in\nu\Phi}\;\textbf{(Step)}}{\vdash s\in\nu\Phi}\;\textbf{(Löb)}$$

Inference Rule

$$\dfrac{C\text{ compatible} \qquad \Delta\vdash t\in C(\nu\Phi)}{\Delta\vdash t\in\nu\Phi}\;\text{(C compatible)}$$

$$C(P\subseteq\mathbb{R}^\omega)=\{1^\omega\oplus s \mid s\in P\}$$

Positive Numbers are Greater Than 0

$$\dfrac{\dfrac{\dfrac{(\text{Def. of } s)\,\dfrac{\dfrac{\dfrac{}{\vdash 1 > 0}}{\vdash s_0 > 0}}{\vdash \blacktriangleright(s_0 > 0)}\,\textbf{(Next)} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\blacktriangleright\varphi \vdash \blacktriangleright\varphi}}{\blacktriangleright\varphi \vdash \blacktriangleright({\color{red}s \in \nu\Phi})}\,\textbf{(Pr)}}{\blacktriangleright\varphi \vdash \blacktriangleright(1^\omega \oplus s \in C(\nu\Phi))}\,{\color{red}(\text{Def. } C)}}{\blacktriangleright\varphi \vdash \blacktriangleright(1^\omega \oplus s \in \nu\Phi)}\,(C\text{ compat.})}{\blacktriangleright\varphi \vdash \blacktriangleright(s' \in \nu\Phi)}\,(\text{Def. of } s)}{\blacktriangleright\varphi \vdash \blacktriangleright(s_0 > 0 \wedge s' \in \nu\Phi)}\,(\blacktriangleright\text{ preserves } \wedge)}{\blacktriangleright\varphi \vdash s \in \nu\Phi}\,\textbf{(Step)}}{\vdash s \in \nu\Phi}\,\textbf{(Löb)}$$

Inference Rule

$$\dfrac{C \text{ compatible} \qquad \Delta \vdash t \in C(\nu\Phi)}{\Delta \vdash t \in \nu\Phi}\,(\text{C compatible})$$

$$C(P \subseteq \mathbb{R}^\omega) = \{1^\omega \oplus s \mid s \in P\}$$

Positive Numbers are Greater Than 0

$$
\dfrac{
\textbf{(Next)}\ \dfrac{\text{(Def. of } s\text{)}\ \dfrac{\dfrac{}{\vdash 1 > 0}}{\vdash s_0 > 0}}{\vdash \blacktriangleright(s_0 > 0)}
\qquad
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\blacktriangleright\varphi \vdash {\color{red}\blacktriangleright\varphi}}}{\blacktriangleright\varphi \vdash \blacktriangleright(s \in \nu\Phi)}\ {\color{red}\textbf{(Pr)}}}{\blacktriangleright\varphi \vdash \blacktriangleright(1^\omega \oplus s \in C(\nu\Phi))}\ \text{(Def. } C\text{)}}{\blacktriangleright\varphi \vdash \blacktriangleright(1^\omega \oplus s \in \nu\Phi)}\ (C \text{ compat.})}{\blacktriangleright\varphi \vdash \blacktriangleright(s' \in \nu\Phi)}\ \text{(Def. of } s\text{)}
}{
\dfrac{\dfrac{\blacktriangleright\varphi \vdash \blacktriangleright(s_0 > 0 \wedge s' \in \nu\Phi)}{\blacktriangleright\varphi \vdash s \in \nu\Phi}\ \textbf{(Step)}}{\vdash s \in \nu\Phi}\ \textbf{(Löb)}
}\ (\blacktriangleright \text{ preserves } \wedge)
$$

Inference Rule

$$
\dfrac{\varphi \in \Delta}{\Delta \vdash \varphi}\ \textbf{(Pr)}
$$

Idea

Extending a Logic

- Given a logic $\mathcal{L}$ with formulas φ and provability $\Gamma \mid \Delta \vdash \varphi$
- Construct a new logic $\overline{\mathcal{L}}$ with the same propositional and first-order connectives, . . .
- . . . and a new connective $\blacktriangleright$, the later modality, that fulfils the axioms for the later modality . . .
- . . . and enables coinductive predicates and up-to techniques

Rules for the later modality

$$\frac{\Gamma \mid \Delta \vdash \varphi}{\Gamma \mid \Delta \vdash \blacktriangleright \varphi}\ \textbf{(Next)} \qquad \frac{\Gamma \mid \Delta \vdash \blacktriangleright(\varphi \to \psi)}{\Gamma \mid \Delta \vdash \blacktriangleright \varphi \to \blacktriangleright \psi}\ \textbf{(Mon)}$$

$$\frac{\Gamma \mid \Delta, \blacktriangleright \varphi \vdash \varphi}{\Gamma \mid \Delta \vdash \varphi}\ \textbf{(Löb)}$$

Extending a Logic

- Given a logic $\mathcal{L}$ with formulas φ and provability $\Gamma \mid \Delta \vdash \varphi$
- Construct a new logic $\overline{\mathcal{L}}$ with the same propositional and first-order connectives, …
- …and a new connective $\blacktriangleright$, the later modality, that fulfils the axioms for the later modality …
- …and enables coinductive predicates and up-to techniques

Rules for coinductive predicates and up-to techniques

$$\frac{\Gamma \mid \Delta \vdash \blacktriangleright(s \in \Phi(\nu\Phi))}{\Gamma \mid \Delta \vdash s \in \nu\Phi} \textbf{ (Step)}$$

(double line)

$$\frac{C \text{ is } \Phi\text{-compatible} \qquad \Gamma \mid \Delta \vdash t \in C(\nu\Phi)}{\Gamma \mid \Delta \vdash t \in \nu\Phi} \textbf{ (Up-to)}$$

Setup

Fibrations

- Fibrations provide abstraction of first- (and higher-)order logic
- $\mathbf{B}$ — Category of typed contexts and terms
- $\mathbf{E}$ — Category of formulas with variables typed in $\mathbf{B}$
- $p\colon \mathbf{E} \to \mathbf{B}$ — functor that assigns to a formula its context

Example

- Set-based predicates: $\mathrm{Pred} \to \mathbf{Set}$
- Quantitative predicates: $\mathrm{qPred} \to \mathbf{Set}$
- Syntactic logic over syntactic terms: $\mathcal{L} \to \mathcal{C}$
- Set-indexed families (dependent types): $\mathrm{Fam}(\mathbf{C}) \to \mathbf{Set}$

Fibrations

- Fibrations provide abstraction of first- (and higher-)order logic
- $\mathbf{B}$ — Category of typed contexts and terms
- $\mathbf{E}$ — Category of formulas with variables typed in $\mathbf{B}$
- $p\colon \mathbf{E} \to \mathbf{B}$ — functor that assigns to a formula its context

Example

- Set-based predicates: $\mathrm{Pred} \to \mathbf{Set}$
- Quantitative predicates: $\mathrm{qPred} \to \mathbf{Set}$
- Syntactic logic over syntactic terms: $\mathcal{L} \to \mathcal{C}$
- Set-indexed families (dependent types): $\mathrm{Fam}(\mathbf{C}) \to \mathbf{Set}$

Example: Quantitative Predicates

Category of quantitative predicates

$$\mathbf{qPred} = \begin{cases} \text{objects:} & (X, \delta) \text{ with } X \in \mathbf{Set} \text{ and } \delta\colon X \to [0,1] \\ \text{morphisms:} & f\colon (X,\delta) \to (Y,\gamma) \text{ if } f\colon X \to Y \text{ in } \mathbf{Set} \\ & \text{ and } \delta \leq \gamma \circ f \end{cases}$$

Reindexing along $u\colon X \to Y$ gives fibration $\mathbf{qPred} \to \mathbf{Set}$

$$u^*(Y,\gamma) = \big(X, \lambda x.\, \gamma(u(x))\big)$$

Products and Exponents

$$(\delta \times \gamma)(x) = \min\{\delta(x), \gamma(x)\}$$

$$\left(\gamma^{\delta}\right)(x) = \begin{cases} 1, & \delta(x) \leq \gamma(x) \\ \gamma(x), & \text{otherwise} \end{cases}$$

Example: Quantitative Predicates

Category of quantitative predicates

$$\mathbf{qPred} = \begin{cases} \text{objects:} & (X,\delta) \text{ with } X \in \mathbf{Set} \text{ and } \delta\colon X \to [0,1] \\ \text{morphisms:} & f\colon (X,\delta) \to (Y,\gamma) \text{ if } f\colon X \to Y \text{ in } \mathbf{Set} \\ & \text{ and } \delta \leq \gamma \circ f \end{cases}$$

Reindexing along $u\colon X \to Y$ gives fibration $\mathbf{qPred} \to \mathbf{Set}$

$$u^*(Y,\gamma) = \big(X, \lambda x.\, \gamma(u(x))\big)$$

Products and Exponents

$$(\delta \times \gamma)(x) = \min\{\delta(x), \gamma(x)\}$$

$$\left(\gamma^{\delta}\right)(x) = \begin{cases} 1, & \delta(x) \leq \gamma(x) \\ \gamma(x), & \text{otherwise} \end{cases}$$

Example: Quantitative Predicates

Category of quantitative predicates

$$\mathbf{qPred} = \begin{cases} \text{objects:} & (X, \delta) \text{ with } X \in \mathbf{Set} \text{ and } \delta \colon X \to [0,1] \\ \text{morphisms:} & f \colon (X, \delta) \to (Y, \gamma) \text{ if } f \colon X \to Y \text{ in } \mathbf{Set} \\ & \text{ and } \delta \leq \gamma \circ f \end{cases}$$

Reindexing along $u \colon X \to Y$ gives fibration $\mathbf{qPred} \to \mathbf{Set}$

$$u^*(Y, \gamma) = \big(X, \lambda x.\, \gamma(u(x))\big)$$

Products and Exponents

$$(\delta \times \gamma)(x) = \min\{\delta(x), \gamma(x)\}$$

$$\left(\gamma^{\delta}\right)(x) = \begin{cases} 1, & \delta(x) \leq \gamma(x) \\ \gamma(x), & \text{otherwise} \end{cases}$$

Coinductive Predicates

Predicate lifting G of behaviour functor F

$$\begin{tikzcd}
\mathbf{E} \arrow[r, "G"] \arrow[d, "p"] & \mathbf{E} \arrow[d, "p"] \\
\mathbf{B} \arrow[r, "F"] & \mathbf{B}
\end{tikzcd}$$

commutes and G preserves Cartesian morphisms.

Predicate transformer for coalgebra $c\colon X \to FX$

$$\Phi := \mathbf{E}_X \xrightarrow{G} \mathbf{E}_{FX} \xrightarrow{c^*} \mathbf{E}_X$$

Coinductive predicate

Final coalgebra $\xi\colon \nu\Phi \to \Phi(\nu\Phi)$ for Φ

ω^{op}-Diagrams in Fibrations

Category of Descending Chains

$$\overline{\mathbf{C}} = [\omega^{\mathrm{op}}, \mathbf{C}] = \text{“category of functors } \omega^{\mathrm{op}} \to \mathbf{C}\text{”}$$

Constant-Index Chains

$$\overline{\mathbf{E}}_X := \overline{\mathbf{E}}_{K_X} \cong \overline{\mathbf{E}_X}$$

If $\sigma \in \overline{\mathbf{E}}_X$, then $p(\sigma_n) = \overline{p}(\sigma)_n = (K_X)_n = X$.

The final chain $\overleftarrow{\Phi} \in \overline{\mathbf{E}}_X$

$$\overleftarrow{\Phi} := \ \mathbf{1} \xleftarrow{\ !\ } \Phi(\mathbf{1}) \xleftarrow{\Phi(!)} \Phi^2(\mathbf{1}) \xleftarrow{\Phi^2(!)} \Phi^3(\mathbf{1}) \xleftarrow{\ \cdots\ }$$

If Φ preserves ω^{op}-limits, then maps $A \to \nu\Phi$ in $\mathbf{E}_X$ can be given by maps $K_A \to \overleftarrow{\Phi}$ in $\overline{\mathbf{E}}_X$.

ω^{op}-Diagrams in Fibrations

Category of Descending Chains

$$\overline{\mathbf{C}} = [\omega^{\mathrm{op}}, \mathbf{C}] = \text{“category of functors } \omega^{\mathrm{op}} \to \mathbf{C}\text{”}$$

Constant-Index Chains

$$\overline{\mathbf{E}}_X := \overline{\mathbf{E}}_{K_X} \cong \overline{\mathbf{E}_X}$$

If $\sigma \in \overline{\mathbf{E}}_X$, then $p(\sigma_n) = \overline{p}(\sigma)_n = (K_X)_n = X$.

The final chain $\overleftarrow{\Phi} \in \overline{\mathbf{E}}_X$

$$\overleftarrow{\Phi} := \ \mathbf{1} \xleftarrow{\ \ !\ \ } \Phi(\mathbf{1}) \xleftarrow{\Phi(!)} \Phi^2(\mathbf{1}) \xleftarrow{\Phi^2(!)} \Phi^3(\mathbf{1}) \xleftarrow{\ \cdots\ }$$

If Φ preserves ω^{op}-limits, then maps $A \to \nu\Phi$ in $\mathbf{E}_X$ can be given by maps $K_A \to \overleftarrow{\Phi}$ in $\overline{\mathbf{E}}_X$.

Greater-Than-0 Example

Example (Predicate lifting and coinductive predicate)

$$F\colon \mathbf{Set} \to \mathbf{Set} \qquad G\colon \mathrm{Pred} \to \mathrm{Pred}$$

$$F = \mathbb{R} \times \mathrm{Id} \qquad G(X, P) = (FX, \{(a, x) \mid a > 0 \land x \in P\})$$

Predicate transformer

$$\Phi = \langle \mathrm{hd}, \mathrm{tl} \rangle^{*} \circ G$$

Coinductive predicate

$$\nu\Phi \subseteq \Phi(\nu\Phi)$$

Example (Notation)

Given a descending chain $\sigma \in \overline{\mathrm{Pred}}_X$, we define

$$\vdash \sigma := \overline{\mathbf{1}}_X \sqsubseteq \sigma \qquad (\iff \text{there exists } \overline{\mathbf{1}}_X \to \sigma)$$

$$x \mathrel{\overline{\in}} \sigma := \sigma^{K_{\{x\}}}$$

$$\vdash s \mathrel{\overline{\in}} \overleftarrow{\Phi} \iff \forall n \in \mathbb{N}.\, s \in \overleftarrow{\Phi}_n \overset{Thm}{\iff} s \in \nu\Phi \iff s \text{ greater t. } 0$$

Greater-Than-0 Example

Example (Predicate lifting and coinductive predicate)

$$F\colon \mathbf{Set} \to \mathbf{Set} \qquad G\colon \mathrm{Pred} \to \mathrm{Pred}$$

$$F = \mathbb{R} \times \mathrm{Id} \qquad G(X, P) = (FX, \{(a, x) \mid a > 0 \wedge x \in P\})$$

Predicate transformer

$$\Phi = \langle \mathrm{hd}, \mathrm{tl} \rangle^* \circ G$$

Coinductive predicate

$$\nu\Phi \subseteq \Phi(\nu\Phi)$$

Example (Notation)

Given a descending chain $\sigma \in \overline{\mathrm{Pred}}_X$, we define

$$\vdash \sigma := \overline{\mathbf{1}}_X \sqsubseteq \sigma \qquad (\iff \text{there exists } \overline{\mathbf{1}}_X \to \sigma)$$

$$x \mathrel{\overline{\in}} \sigma := \sigma^{K_{\{x\}}}$$

$$\vdash s \mathrel{\overline{\in}} \overleftarrow{\Phi} \iff \forall n \in \mathbb{N}.\, s \in \overleftarrow{\Phi}_n \overset{Thm}{\iff} s \in \nu\Phi \iff s \text{ greater t. } 0$$

Later Modality

Theorem

For each $c \in \overline{\mathbf{B}}$*, there is a fibred functor* $\blacktriangleright^c \colon \overline{\mathbf{E}}_c \to \overline{\mathbf{E}}_c$*.*

- $\blacktriangleright^c$ *preserves fibred finite products*
- $\blacktriangleright^c$ *preserves all fibred limits if* p *is a bifibration*
- *there is a natural transformation* $\mathrm{next}^c \colon \mathrm{Id} \Rightarrow \blacktriangleright^c$

Associated proof rules

$$\frac{f\colon \tau \to \sigma}{\blacktriangleright f\colon \blacktriangleright \tau \to \blacktriangleright \sigma}\ \textbf{(Mon)} \qquad \frac{f\colon \tau \to \sigma}{\mathrm{next}^c \circ f\colon \tau \to \blacktriangleright^c \sigma}\ \textbf{(Next)}$$

Later Modality

Theorem

For each $c \in \overline{\mathbf{B}}$*, there is a fibred functor* $\blacktriangleright^c \colon \overline{\mathbf{E}}_c \to \overline{\mathbf{E}}_c$*.*

- $\blacktriangleright^c$ *preserves fibred finite products*
- $\blacktriangleright^c$ *preserves all fibred limits if* p *is a bifibration*
- *there is a natural transformation* $\mathrm{next}^c \colon \mathrm{Id} \Rightarrow \blacktriangleright^c$

Associated proof rules

$$\frac{f \colon \tau \to \sigma}{\blacktriangleright f \colon \blacktriangleright \tau \to \blacktriangleright \sigma}\ \textbf{(Mon)} \qquad \frac{f \colon \tau \to \sigma}{\mathrm{next}^c \circ f \colon \tau \to \blacktriangleright^c \sigma}\ \textbf{(Next)}$$

The Löb Rule

Theorem

If $p \colon \mathbf{E} \to \mathbf{B}$ has fibred finite limits and exponents, then also $\overline{p} \colon \overline{\mathbf{E}} \to \overline{\mathbf{B}}$ does.
Notation: for $\sigma, \tau \in \overline{\mathbf{E}}_c$ have $\sigma^\tau \in \overline{\mathbf{E}}_c$.

Theorem

For every $\sigma \in \overline{\mathbf{E}}_c$ there is a unique map in $\overline{\mathbf{E}}_c$, dinatural in σ,

$$\mathrm{l\ddot{o}b}^c_\sigma \colon \sigma^{\blacktriangleright^c \sigma} \to \sigma.$$

Associated proof rule

$$\frac{f \colon \tau \times \blacktriangleright^c \sigma \to \sigma}{\mathrm{l\ddot{o}b}^c_\sigma \circ \lambda f \colon \tau \to \sigma}\ \textbf{(Löb)}$$

The Löb Rule

Theorem

If $p \colon \mathbf{E} \to \mathbf{B}$ *has fibred finite limits and exponents, then also* $\overline{p} \colon \overline{\mathbf{E}} \to \overline{\mathbf{B}}$ *does.*

Notation: for $\sigma, \tau \in \overline{\mathbf{E}}_c$ *have* $\sigma^\tau \in \overline{\mathbf{E}}_c$*.*

Theorem

For every $\sigma \in \overline{\mathbf{E}}_c$ *there is a unique map in* $\overline{\mathbf{E}}_c$*, dinatural in* σ*,*

$$\mathrm{l\ddot{o}b}^c_\sigma \colon \sigma^{\blacktriangleright^c \sigma} \to \sigma.$$

Associated proof rule

$$\frac{f \colon \tau \times \blacktriangleright^c \sigma \to \sigma}{\mathrm{l\ddot{o}b}^c_\sigma \circ \lambda f \colon \tau \to \sigma} \textbf{ (Löb)}$$

Steps on the Final Chain

Theorem

$\overleftarrow{\Phi} = \blacktriangleright\left(\overline{\Phi}\,\overleftarrow{\Phi}\right)$, *where* $\blacktriangleright := \blacktriangleright^{K_X}$.

Associated proof rule

$$\frac{f : \tau \to \blacktriangleright\left(\overline{\Phi}\,\overleftarrow{\Phi}\right)}{f : \tau \to \overleftarrow{\Phi}}\;\textbf{(Step)}$$

Steps on the Final Chain

Theorem

$\overleftarrow{\Phi} = \blacktriangleright\left(\overline{\Phi}\,\overleftarrow{\Phi}\right)$, *where* $\blacktriangleright := \blacktriangleright^{K_X}$.

Associated proof rule

$$\frac{f : \tau \to \blacktriangleright\left(\overline{\Phi}\,\overleftarrow{\Phi}\right)}{f : \tau \to \overleftarrow{\Phi}}\ \textbf{(Step)}$$

Up-To Techniques

Theorem

For $T\colon \mathbf{E}_X \to \mathbf{E}_X$ *and* $\rho\colon T\Phi \Rightarrow \Phi T$, *there is* $\overleftarrow{\rho} : \overline{T}\,\overleftarrow{\Phi} \to \overleftarrow{\Phi}$.

Associated proof rule

$$\frac{f : \tau \to \overline{T}\,\overleftarrow{\Phi} \qquad \rho\colon T\Phi \Rightarrow \Phi T \ (T \text{ compatible})}{\overleftarrow{\rho} \circ f : \tau \to \overleftarrow{\Phi}}\ \textbf{(Up-to)}$$

Up-To Techniques

Theorem

For $T\colon \mathbf{E}_X \to \mathbf{E}_X$ *and* $\rho\colon T\Phi \Rightarrow \Phi T$*, there is* $\overleftarrow{\rho} : \overline{T}\,\overleftarrow{\Phi} \to \overleftarrow{\Phi}$*.*

Associated proof rule

$$\frac{f : \tau \to \overline{T}\,\overleftarrow{\Phi} \qquad \rho\colon T\Phi \Rightarrow \Phi T \ (T \text{ compatible})}{\overleftarrow{\rho} \circ f : \tau \to \overleftarrow{\Phi}} \ \textbf{(Up-to)}$$

Quantifiers (Products & Coproducts)

Theorem

If for $u\colon I \to J$ in $\mathbf{B}$ the coproduct $\coprod_u\colon \mathbf{E}_I \to \mathbf{E}_J$ along u exists, then the coproduct $\coprod_{\overline{u}}\colon \overline{\mathbf{E}}_I \to \overline{\mathbf{E}}_J$ along $\overline{u}\colon K_I \to K_J$ is given by $\overline{\coprod_u}$. Similarly, the product $\prod_{\overline{u}}$ along $\overline{u}$ is given by $\overline{\prod_u}$.

Associated proof rule

Let $\pi\colon I \times J \to I$, and write $W = \overline{\pi}^*$ for weakening $W\colon \overline{\mathbf{E}}_I \to \overline{\mathbf{E}}_{I\times J}$ and $\forall_J = \prod_{\overline{\pi}}\colon \overline{\mathbf{E}}_{I\times J} \to \overline{\mathbf{E}}_I$. Then

$$\begin{array}{rc} f\colon & W\tau \longrightarrow \sigma \\ \hline\hline \check{f}\colon & \tau \longrightarrow \forall_J\, \sigma \end{array}$$

Quantifiers (Products & Coproducts)

Theorem

If for $u \colon I \to J$ *in* $\mathbf{B}$ *the coproduct* $\coprod_u \colon \mathbf{E}_I \to \mathbf{E}_J$ *along* u *exists, then the coproduct* $\coprod_{\overline{u}} \colon \overline{\mathbf{E}}_I \to \overline{\mathbf{E}}_J$ *along* $\overline{u} \colon K_I \to K_J$ *is given by* $\overline{\coprod_u}$. *Similarly, the product* $\prod_{\overline{u}}$ *along* $\overline{u}$ *is given by* $\overline{\prod_u}$.

Associated proof rule

Let $\pi \colon I \times J \to I$, and write $W = \overline{\pi}^*$ for weakening $W \colon \overline{\mathbf{E}}_I \to \overline{\mathbf{E}}_{I \times J}$ and $\forall_J = \prod_{\overline{\pi}} \colon \overline{\mathbf{E}}_{I \times J} \to \overline{\mathbf{E}}_I$. Then

$$\frac{f\colon \quad W\tau \longrightarrow \sigma}{\check{f}\colon \qquad \tau \longrightarrow \forall_J\, \sigma}$$

Conclusion

Related Systems

- Parameterised coinduction — only for lattices; works on fixed points
- CIRC — cyclic proof system for coinductive predicates; hard to understand and hand-crafted
- Cyclic proof systems — purely syntactic (??), hence have to be hand-crafted; rely on global correctness conditions
- (Bisimulation) Games — also rely on global parity conditions; proof steps in presented system can be seen as challenge-response pairs
- Step-indexed relations – instance of this and the framework by Birkedal et al.

Extensions and Future Directions

- Preprint: ArXiv 1802.07143
- Publication with more examples etc. under review
- Extend to larger ordinals; the CCC result is already general, the results about the final chain need work:

$$(\blacktriangleright \sigma)_\alpha = \lim_{\beta<\alpha} \sigma_\beta$$

- Properly apply to motivating, syntactic example; possibly by automatically extracting a syntactic logic
- Can we construct other recursive proof systems in fibrations? (Later with clocks, cyclic proof systems, . . .)

Thank you very much for your attention!

Diagrams are Fibred CCCs

Intuition from Kripke models

$$W, w \vDash \varphi \to \psi \quad \iff \quad \forall w \leq v.\, W, v \vDash \varphi \text{ implies } W, v \vDash \psi$$

Implication for sequences of formulas

Let $\{\varphi_n\}_{n \in \omega^{\mathrm{op}}}$ and $\{\psi_n\}_{n \in \omega^{\mathrm{op}}}$ be sequences of formulas. Define

$$(\psi \Rightarrow \varphi)_n := \bigwedge_{m \leq n} \psi_m \to \varphi_n,$$

General Exponentials

The exponential object of $\sigma, \tau \in \overline{\mathbf{E}}_c$ is given by the end

$$(\tau^\sigma)(n) = \int_{m \leq n} \big(c(m \leq n)^* \, \tau(m)\big)^{c(m \leq n)^* \, \sigma(m)}.$$

Diagrams are Fibred CCCs

Intuition from Kripke models

$$W, w \vDash \varphi \to \psi \quad \iff \quad \forall w \leq v.\, W, v \vDash \varphi \text{ implies } W, v \vDash \psi$$

Implication for sequences of formulas

Let $\{\varphi_n\}_{n \in \omega^{\mathrm{op}}}$ and $\{\psi_n\}_{n \in \omega^{\mathrm{op}}}$ be sequences of formulas. Define

$$(\psi \Rightarrow \varphi)_n := \bigwedge_{m \leq n} \psi_m \to \varphi_n,$$

General Exponentials

The exponential object of $\sigma, \tau \in \overline{\mathbf{E}}_c$ is given by the end

$$(\tau^{\sigma})(n) = \int_{m \leq n} \big(c(m \leq n)^* \, \tau(m)\big)^{c(m \leq n)^* \, \sigma(m)}.$$

Diagrams are Fibred CCCs

Intuition from Kripke models

$$W, w \vDash \varphi \to \psi \quad\iff\quad \forall w \leq v.\, W, v \vDash \varphi \text{ implies } W, v \vDash \psi$$

Implication for sequences of formulas

Let $\{\varphi_n\}_{n\in\omega^{\mathrm{op}}}$ and $\{\psi_n\}_{n\in\omega^{\mathrm{op}}}$ be sequences of formulas. Define

$$(\psi \Rightarrow \varphi)_n := \bigwedge_{m\leq n} \psi_m \to \varphi_n,$$

General Exponentials

The exponential object of $\sigma, \tau \in \overline{\mathbf{E}}_c$ is given by the end

$$(\tau^\sigma)(n) = \int_{m\leq n} \big(c(m \leq n)^* \, \tau(m)\big)^{c(m\leq n)^* \, \sigma(m)}.$$

Recursive Logic

Later Modality

Theorem

For each $c \in \overline{\mathbf{B}}$*, there is a fibred functor* $\blacktriangleright^c \colon \overline{\mathbf{E}}_c \to \overline{\mathbf{E}}_c$ *given by*

$$\begin{aligned}(\blacktriangleright^c \sigma)_0 &= \mathbf{1}_{c_0}\\(\blacktriangleright^c \sigma)_{n+1} &= c(n \leq n+1)^*(\sigma_n).\end{aligned}$$

- $\blacktriangleright^c$ *preserves fibred finite products*
- $\blacktriangleright^c$ *preserves all fibred limits if* p *is a bifibration*
- *there is a natural transformation* $\mathrm{next}^c \colon \mathrm{Id} \Rightarrow \blacktriangleright^c$

Associated proof rules

$$\frac{f \colon \tau \to (\blacktriangleright^c \sigma) \times (\blacktriangleright^c \sigma')}{\check{f} \colon \tau \to \blacktriangleright^c(\sigma \times \sigma')} \qquad \frac{f \colon \tau \to \sigma}{\mathrm{next}^c \circ f \colon \tau \to \blacktriangleright^c \sigma}$$

Later Modality

Theorem

For each $c \in \overline{\mathbf{B}}$*, there is a fibred functor* $\blacktriangleright^c \colon \overline{\mathbf{E}}_c \to \overline{\mathbf{E}}_c$ *given by*

$$\begin{aligned}(\blacktriangleright^c \sigma)_0 &= \mathbf{1}_{c_0} \\ (\blacktriangleright^c \sigma)_{n+1} &= c(n \leq n+1)^*(\sigma_n).\end{aligned}$$

- $\blacktriangleright^c$ *preserves fibred finite products*
- $\blacktriangleright^c$ *preserves all fibred limits if* p *is a bifibration*
- *there is a natural transformation* $\mathrm{next}^c \colon \mathrm{Id} \Rightarrow \blacktriangleright^c$

Associated proof rules

$$\frac{f \colon \tau \to (\blacktriangleright^c \sigma) \times (\blacktriangleright^c \sigma')}{\check{f} \colon \tau \to \blacktriangleright^c(\sigma \times \sigma')} \qquad \frac{f \colon \tau \to \sigma}{\mathrm{next}^c \circ f \colon \tau \to \blacktriangleright^c \sigma}$$