Recursive Proofs for Coinductive Predicates in Fibrations

Henning Basold[1]

CNRS, ENS Lyon, henning.basold@ens-lyon.fr

The usual way to prove that some objects are contained in a coinductive predicate or are related by a coinductive relation, is to establish an invariant. Suppose $\Phi\colon L \to L$ is a monotone function on a lattice and Φ that has a greatest fixed point $\nu\Phi$. One proves that the coinductive predicate $\nu\Phi$ holds for $x \in L$ by establishing a $y \in L$ with $x \leq y \leq \Phi(y)$. This approach does, however, not fit common practice, as one usually incrementally constructs the invariant y, rather than guessing it, while following the necessary proof steps. Such an incremental construction leads to a recursive proof methodology. We will focus on here on recursive proofs, in which recursion is controlled by using the so-called later modality [4]. This allows checking of recursive proofs on a per-rule basis and gives a per-rule soundness proof. Birkedal et al. [3] have studied the later modality for ω^{op}-chains in the category **Set** of sets. Since **Set** provides a very rich setting for higher-order logic, one can encode most propositions and proofs in that category. However, syntactic presentations get lost this way and quantitative reasoning is not available there. Thus, we aim to extend an arbitrary (syntactic) logic with a later modality, independently of the presentation of the logic. In fact, the syntactic first-order logic given by the author in [2] to reason about program equivalences is an instance of such an extension.

In this talk, we will develop recursive proofs for a general first-order logic, given in form of a fibration. This way, we obtain recursive proofs for coinductive predicates in as diverse settings as set-based predicates, quantitative predicates, syntactic first-order logic, and dependent type theory. Fibrations provide a good basis, since they allow us to deal abstractly with formulas that contain typed variables. More precisely, let $p\colon \mathbf{E} \to \mathbf{B}$ be functor. For $I \in \mathbf{B}$, we let $\mathbf{E}_I$ be the *fibre (category) above* I that has objects $X \in \mathbf{E}$ with $p(X) = I$ and morphisms $f\colon X \to Y$ that fulfil $p(f) = \mathrm{id}_I$. A *(cloven) fibration* is a functor $p\colon \mathbf{E} \to \mathbf{B}$, such that for every morphism $u\colon I \to J$ in $\mathbf{B}$ there is a *reindexing functor* $u^*\colon \mathbf{E}_J \to \mathbf{E}_I$ with isomorphisms $\mathrm{id}_I^* \cong \mathrm{Id}_{\mathbf{E}_I}$ and $u \circ v^* \cong v^* \circ u^*$ that fulfil certain coherence conditions. To implement recursion, we will require that p is a *fibred Cartesian closed category* (*fibred CCCs*), which means that every fibre $\mathbf{E}_I$ has finite products and exponential objects that are preserved by reindexing.

In our study of the later modality, we proceed as follows. Given a category $\mathbf{B}$, an ω^{op}-*chain* in $\mathbf{B}$ is a functor $c\colon \omega^{\mathrm{op}} \to \mathbf{B}$, and we denote by $\overline{\mathbf{B}}$ the functor category $[\omega^{\mathrm{op}}, \mathbf{B}]$ that has chains as objects and natural transformations as morphisms. We show how to obtain from a fibration $p\colon \mathbf{E} \to \mathbf{B}$ a fibration $\overline{p}\colon \overline{\mathbf{E}} \to \overline{\mathbf{B}}$ of ω^{op}-chains. In this fibration, we can define for each chain $c\colon \omega^{\mathrm{op}} \to \mathbf{B}$ the later modality as a fibred functor $\blacktriangleright\colon \overline{\mathbf{E}}_c \to \overline{\mathbf{E}}_c$ and its unit $\mathrm{next}\colon \mathrm{Id} \Rightarrow \blacktriangleright$. That this functor is fibred intuitively means that substitutions

distribute over the later modality via $\mathrm{subst}_\sigma \colon u^*(\blacktriangleright\sigma) \cong \blacktriangleright(u^*\sigma)$. The functor $\blacktriangleright$ also preserves fibred (finite) products. To be able to express and solve fixed point equations we need exponential objects, because for an ω^{op}-chain σ in $\mathbf{E}$, the solutions of contractive fixed point equations on σ are given by a morphism $\mathrm{löb}_\sigma \colon \sigma^{\blacktriangleright\sigma} \to \sigma$, cf. [3]. Thus, in the next step we show that the fibration $\overline{p}$ is a fibred CCC and that the morphism $\mathrm{löb}_\sigma$ exists for each σ, that löb is dinatural in σ and that it can be used to solve contractive equations. These constructions are summed up in the rules below, where we leave standard category theoretical constructions and all equations out.

$$\frac{f \colon \tau \to \sigma}{\blacktriangleright f \colon \blacktriangleright\tau \to \blacktriangleright\sigma} \qquad \frac{f \colon \tau \to \blacktriangleright\sigma \times \blacktriangleright\delta}{\iota^{-1} \circ f \colon \tau \to \blacktriangleright(\sigma \times \delta)} \qquad \frac{f \colon \tau \to \blacktriangleright(u^*\sigma)}{\mathrm{subst}_\sigma^{-1} \circ f \colon \tau \to u^*(\blacktriangleright\sigma)}$$

$$\frac{f \colon \tau \to \sigma}{\mathrm{next}_\sigma \circ f \colon \tau \to \blacktriangleright\sigma} \qquad \frac{f \colon \tau \times \blacktriangleright\sigma \to \sigma}{\mathrm{löb}_\sigma \circ \lambda f \colon \tau \to \sigma}$$

Above, we described the later modality and solutions to fixed point equations in general. The reason for introducing all this machinery is to be able to construct morphisms into coinductive predicates. Let $X \in \mathbf{B}$, we denote by $\overline{\mathbf{E}}_X$ the fibre above the constant chain K_X. A *coinductive predicate* is a final coalgebra $\nu\Phi$ for a functor $\Phi \colon \overline{\mathbf{E}}_X \to \overline{\mathbf{E}}_X$. If $\nu\Phi$ can be constructed as limit of the ω^{op}-chain $\overleftarrow{\Phi}$, then morphisms $\psi \to \nu\Phi$ in $\mathbf{E}_X$ are equivalently given by morphisms $K_\psi \to \overleftarrow{\Phi}$ in $\overline{\mathbf{E}}_X$. Moreover, if we write $\overline{\Phi}$ for the point-wise application of Φ, then we have $\overleftarrow{\Phi} = \blacktriangleright\left(\overline{\Phi}\,\overleftarrow{\Phi}\right)$. Finally, given a functor $T \colon \overline{\mathbf{E}}_X \to \overline{\mathbf{E}}_X$, we say that T is *Φ-compatible* if there is a natural transformation $\rho \colon T\Phi \Rightarrow \Phi T$. For a compatible T, it is easy to construct a morphism $\overleftarrow{\rho} \colon \overline{T}\left(\overleftarrow{\Phi}\right) \to \overleftarrow{\Phi}$. Putting all of this together, we obtain the following rules.

$$\frac{K_\psi \to \overleftarrow{\Phi}}{\psi \to \nu\Phi} \qquad \frac{f \colon \tau \to \blacktriangleright\left(\overline{\Phi}\,\overleftarrow{\Phi}\right)}{f \colon \tau \to \overleftarrow{\Phi}} \qquad \frac{f \colon \tau \to \overline{T}\,\overleftarrow{\Phi} \qquad \rho \colon T\Phi \Rightarrow \Phi T \ (T \text{ compatible})}{\overleftarrow{\rho} \circ f \colon \tau \to \overleftarrow{\Phi}}$$

In the talk, I will explain all the above, the lifting of quantifiers to $\overline{p} \colon \overline{\mathbf{E}} \to \overline{\mathbf{B}}$, and give some illustrative examples. Further details can be found in [1].

References

1. Basold, H.: Breaking the Loop: Recursive Proofs for Coinductive Predicates in Fibrations. ArXiv e-prints (Feb 2018), https://arxiv.org/abs/1802.07143
2. Basold, H.: Mixed Inductive-Coinductive Reasoning: Types, Programs and Logic. PhD Thesis, Radboud University, Nijmegen (2018), https://perso.ens-lyon.fr/henning.basold/thesis/
3. Birkedal, L., Møgelberg, R.E., Schwinghammer, J., Støvring, K.: First steps in synthetic guarded domain theory: Step-indexing in the topos of trees. Logical Methods in Computer Science 8(4) (2012), https://doi.org/10.2168/LMCS-8(4:1)2012
4. Nakano, H.: A Modality for Recursion. In: LICS. pp. 255–266. IEEE Computer Society (2000), https://doi.org/10.1109/LICS.2000.855774