Solving Guarded Domain Equations in Presheaves Over Ordinals and Mechanizing It

Sergei Stepanenko and Amin Timany

Aarhus University, Aarhus, Denmark
{sergei.stepanenko, timany}@cs.au.dk

1 Introduction

Finding solutions to so-called recursive domain equations [11] is a well-known, important problem in the study of programs and programming languages. Mathematically speaking, the problem is finding a fixed point (up to isomorphism) of a suitable endo-functor $F : \mathcal{C} \to \mathcal{C}$ on a suitable category $\mathcal{C}$, *i.e.*, an object X of $\mathcal{C}$ such that $F(X) \simeq X$ [9, 8, 11, 14, 1, 4]. A particularly useful instance, inspired by the step-indexing technique, is where the functor is over (a subcategory of) the category of presheaves over the ordinal ω and the functors are locally-contractive, also known as *guarded functors* [3]. This corresponds to step-indexing over natural numbers. However, for certain problems, *e.g.*, when dealing with infinite non-determinism, one needs to employ trans-finite step-indexing, *i.e.*, consider presheaf categories over higher ordinals [2, 5]. Prior work on trans-finite step-indexing either only considers a very narrow class of functors over a particularly restricted subcategory of presheaves over higher ordinals [12], or treats the problem very generally working with sheaves over an arbitrary complete Heyting algebra with a well-founded basis [3]. In this work we present a solution to the guarded domain equations problem over *all* so-called guarded functors over the category of *presheaves* over ordinal numbers, as well as its mechanization in the Rocq prover. This can be seen as a simplification of the work of Birkedal *et al.* [3] from the setting of the category of sheaves to the setting of the category of presheaves which is more amenable to mechanization using proof assistants. Our Rocq mechanization [13] can be found at: https://github.com/logsem/synthetic_domains.

2 Presheaves Over All Ordinals

In this work we talk about step-indexing over (all) ordinals, *e.g.*, we speak of sheaves or presheaves over **Ord**, the set of all ordinals (which we also consider to be a preorder category under the usual order). This is to be understood as the set of all ordinals definable in a certain Grothendieck universe. (In Rocq, the type **Ord** is a universe polymorphic definition corresponding to the type of all ordinals in the universe.)

An important endo-functor on $\mathbf{PSh}(\mathbf{Ord})$ that plays an important role in our development is the so-called later functor ($\blacktriangleright : \mathbf{PSh}(\mathbf{Ord}) \to \mathbf{PSh}(\mathbf{Ord})$):

$$\blacktriangleright F(\alpha) := \lim_{\beta \prec \alpha} F(\beta) \qquad\qquad (\blacktriangleright F)_{\beta \preceq \alpha} := \lim_{\gamma \prec \beta} \Pi_{\gamma}^{\blacktriangleright F(\alpha)}$$

The object map of $\blacktriangleright$, at each stage, takes the limit (in **Set**) of the diagram induced by the object (presheaf) it is mapping at all smaller stages. In particular, $\blacktriangleright F(0)$ is always the terminal (singleton) set, and $\blacktriangleright F(\alpha^{+}) \simeq F(\alpha)$. The morphism map of the functor $\blacktriangleright$, $(\blacktriangleright F)_{\beta \preceq \alpha}$ is defined as the amalgamation of projections $\Pi_{\gamma}^{\blacktriangleright F(\alpha)} : \blacktriangleright F(\alpha) \to F(\gamma)$ of the limit that is $(\blacktriangleright F)(\alpha)$. There is also an important natural transformation $\mathsf{Next} : \mathsf{id}_{\mathbf{PSh}(\mathbf{Ord})} \to \blacktriangleright$ associated with $\blacktriangleright$.

We say a morphism in $\mathbf{PSh}(\mathbf{Ord})$, *i.e.*, a natural transformation $\eta : F \to G$, is contractive, if it factors through Next, *i.e.*, $\eta = \eta' \circ \mathsf{Next}_F$; we call η' the witness of contractivity. Contractive morphisms are closed under composition with any other (not necessarily contractive) natural transformation. Importantly, contractive natural transformations have *unique* fixed points; a natural transformation $\xi : 1 \to A$ is a fixed point of a contractive morphism $\eta : A \to A$ if $\eta \circ \xi = \xi$.

3 Locally Contractive Functors and Solutions

Definition (Locally Contractive Functors)**.** *Let $\mathcal{C}$ and $\mathcal{D}$ be two $\mathbf{PSh}(\mathbf{Ord})$-enriched categories. We write $\mathbb{E}^{\mathsf{hom}_{\mathcal{C}}}_{A,B}$ for the object of $\mathbf{PSh}(\mathbf{Ord})$ representing the collection of morphisms from A to B in a category $\mathcal{C}$, and we write $\mathbb{E}^{\mathsf{hm}_F}_{A,B} : \mathbb{E}^{\mathsf{hom}_{\mathcal{C}}}_{A,B} \to \mathbb{E}^{\mathsf{hom}_{\mathcal{D}}}_{F(A),F(B)}$ for the morphism of $\mathbf{PSh}(\mathbf{Ord})$ representing the internal action of an enriched functor F on morphisms. We say a $\mathbf{PSh}(\mathbf{Ord})$-enriched functor $F : \mathcal{C} \to \mathcal{D}$ is locally contractive if the internal action morphisms of F, $\mathbb{E}^{\mathsf{hm}_F}_{A,B}$, are contractive with the witness of contractivity being morphisms $\mathbb{E}^{\blacktriangleright\mathsf{hm}_F}_{A,B} : \blacktriangleright \mathbb{E}^{\mathsf{hom}_{\mathcal{C}}}_{A,B} \to \mathbb{E}^{\mathsf{hom}_{\mathcal{D}}}_{F(A),F(B)}$. Furthermore, expressed in terms of equality of morphisms in $\mathbf{PSh}(\mathbf{Ord})$, the morphisms $\mathbb{E}^{\blacktriangleright\mathsf{hm}_F}_{A,B}$ must preserve identity and composition.*

Importantly, the functor $\blacktriangleright$ itself (under self-enrichment of $\mathbf{PSh}(\mathbf{Ord})$) is locally contractive, and locally contractive functors are closed under composition with arbitrary enriched functors.

Theorem. *Any locally contractive functor $F : \mathcal{C} \to \mathcal{C}$ has a unique (up to isomorphism) solution X for which $F(X) \simeq X$.*

Note how each solution $F(X) \simeq X$ gives rise to an F-algebra structure on X. The proof of uniqueness of the solution essentially shows that an object is a solution if and only if it is the initial F-algebra — the F-algebra morphism out of this initial F-algebra is constructed as the unique fixed point of the internal action of the functor F on morphisms, which is contractive since F is locally contractive. It is also for this reason that our construction of the solution is essentially constructing an F-algebra whose underlying map is an isomorphism. Technically, this construction consists of iteratively (by transfinite induction) constructing ordinal-shaped diagrams of F-algebras, taking their limit, and applying F to the constructed limit.

Apart from working with the category of F-algebras as opposed to working directly in $\mathcal{C}$, our solution construction differs from that of Birkedal *et al.* [3] in how we treat zero and limit ordinals. Working with sheaves, Birkedal *et al.* [3] at zero and limit ordinals simply take the limit of the construction at stages below. By contrast, we apply F to the limit at every single stage and not just at successor ordinals. (A similar difference also appears in our construction of fixed points of contractive morphisms as defined above.) Another way to look at this difference is if we look at the sequence of objects constructed in these two approaches (in our case the carrier objects of the algebras we compute). Up to isomorphism, what we compute is the sequence X while Birkedal *et al.* [3] compute the sequence Y:

$$\begin{array}{llllll} X_0 := F(1); & X_1 := F(F(1)); & X_2 := F(F(F(1))); & \cdots & X_\omega := F(\lim_{\alpha \prec \omega} X_\alpha); & X_{\omega^+} := F(X_\omega); \quad \cdots \\ Y_0 := 1; & Y_1 := F(1); & Y_2 := F(F(1)); & \cdots & Y_\omega := \lim_{\alpha \prec \omega} Y_\alpha; & Y_{\omega^+} := F(Y_\omega); \quad \cdots \end{array}$$

4 Related Work

The most closely related works to us are Rocq mechanizations of the domain equation solver of the ModuRes library [10], the domain equation solver of the Iris program logic [6] which is a nicer reimplementation of the domain equation solver of the ModuRes library, and the domain equation solver of transfinite Iris [12]. (In fact, for our mechanization we have used the step-indexing development of Spies *et al.* [12] who use the mechanization of ordinal numbers by Kirst *et al.* [7].) The former two mechanizations work with the category of complete ordered family of equivalences (COFEs), a representation of the category of complete bisected bounded ultra metric spaces (CBUlt) [4] that is particularly amenable to mechanizations [10]. These only support step-indexing up to ω. Transfinite Iris, inspired by Birkedal *et al.* [3], extends the definition of OFEs (COFEs without completeness requirement) and COFEs to higher ordinals. However, Transfinite Iris, unlike the ModuRes library and Iris, only solves domain equations for functors of the form $\mathrm{OFE}^{\mathsf{op}} \times \mathrm{OFE} \to \mathrm{COFE}$ and not $\mathrm{COFE}^{\mathsf{op}} \times \mathrm{COFE} \to \mathrm{COFE}$.

References

[1] Pierre America and Jan J. M. M. Rutten. Solving Reflexive Domain Equations in a Category of Complete Metric Spaces. *J. Comput. Syst. Sci.*, 39(3):343–375, 1989.

[2] Lars Birkedal, Ales Bizjak, and Jan Schwinghammer. Step-Indexed Relational Reasoning for Countable Nondeterminism. *Log. Methods Comput. Sci.*, 9(4), 2013.

[3] Lars Birkedal, Rasmus Ejlers Møgelberg, Jan Schwinghammer, and Kristian Støvring. First Steps in Synthetic Guarded Domain Theory: Step-Indexing in the Topos of Trees. In *Proceedings of the 26th Annual IEEE Symposium on Logic in Computer Science, LICS 2011, June 21-24, 2011, Toronto, Ontario, Canada*, pages 55–64. IEEE Computer Society, 2011.

[4] Lars Birkedal, Kristian Støvring, and Jacob Thamsborg. The category-theoretic solution of recursive metric-space equations. *Theor. Comput. Sci.*, 411(47):4102–4122, 2010.

[5] Ales Bizjak, Lars Birkedal, and Marino Miculan. A Model of Countable Nondeterminism in Guarded Type Theory. In Gilles Dowek, editor, *Rewriting and Typed Lambda Calculi - Joint International Conference, RTA-TLCA 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 14-17, 2014. Proceedings*, volume 8560 of *Lecture Notes in Computer Science*, pages 108–123. Springer, 2014.

[6] Ralf Jung, Robbert Krebbers, Lars Birkedal, and Derek Dreyer. Higher-order ghost state. In Jacques Garrigue, Gabriele Keller, and Eijiro Sumii, editors, *Proceedings of the 21st ACM SIGPLAN International Conference on Functional Programming, ICFP 2016, Nara, Japan, September 18-22, 2016*, pages 256–269. ACM, 2016.

[7] Dominik Kirst and Gert Smolka. Large model constructions for second-order ZF in dependent type theory. In June Andronick and Amy P. Felty, editors, *Proceedings of the 7th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2018, Los Angeles, CA, USA, January 8-9, 2018*, pages 228–239. ACM, 2018.

[8] Dana Scott. Outline of a mathematical theory of computation. Technical Report PRG02, OUCL, November 1970.

[9] Dana Scott. Continuous lattices. In F. W. Lawvere, editor, *Toposes, Algebraic Geometry and Logic*, pages 97–136, Berlin, Heidelberg, 1972. Springer Berlin Heidelberg.

[10] Filip Sieczkowski, Ales Bizjak, and Lars Birkedal. ModuRes: A Coq Library for Modular Reasoning About Concurrent Higher-Order Imperative Programming Languages. In Christian Urban and Xingyuan Zhang, editors, *Interactive Theorem Proving - 6th International Conference, ITP 2015, Nanjing, China, August 24-27, 2015, Proceedings*, volume 9236 of *Lecture Notes in Computer Science*, pages 375–390. Springer, 2015.

[11] Michael B. Smyth and Gordon D. Plotkin. The Category-Theoretic Solution of Recursive Domain Equations. *SIAM J. Comput.*, 11(4):761–783, 1982.

[12] Simon Spies, Lennard Gäher, Daniel Gratzer, Joseph Tassarotti, Robbert Krebbers, Derek Dreyer, and Lars Birkedal. Transfinite Iris: resolving an existential dilemma of step-indexed separation

logic. In Stephen N. Freund and Eran Yahav, editors, *PLDI '21: 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation, Virtual Event, Canada, June 20-25, 2021*, pages 80–95. ACM, 2021.

[13] Sergei Stepanenko and Amin Timany. The Rocq Mechanization of Solving Guarded Domain Equations in Presheaves Over Ordinals. `https://github.com/logsem/synthetic_domains`.

[14] Mitchell Wand. Fixed-Point Constructions in Order-Enriched Categories. *Theor. Comput. Sci.*, 8:13–30, 1979.