Substructural Weakest Preconditions in Fibrations

1 Introduction

Hoare triples mediate between logic and computation, so their interpretation plays a key role in the semantics of separation logic. Modern separation logics express their Hoare triples in terms of a *weakest precondition modality*. Often, the most difficult part of developing a separation logic is finding a weakest precondition modality that is computationally adequate in an appropriate sense while still supporting compositional proof rules. In the presence of effects and resources, there is often no canonical choice for the weakest precondition modality, but the design space for these modalities remains underexplored. Existing theoretical work on separation logic concentrates on the logic of bunched implications (BI) and its higher-order extensions [2–4, 7–9], while theoretical studies of weakest preconditions have only dealt with structural logics [1, 5, 10, 11].

In this work-in-progress talk, we attempt to provide a theory of weakest preconditions for separation logics by viewing them as liftings of a monad T from a category of types C to a category of predicates $\hat{C}$ fibered over C. Our approach follows Aguirre and Katsumata [1], who developed a theory of structural weakest preconditions in terms of monad liftings. We test our new approach by exhibiting a standard separation logic for heap-manipulating programs as a monad lifting. We will also describe a construction for obtaining new monad liftings from old.

2 Background

We recall the results of Aguirre and Katsumata [1] that we adapt to the substructural setting.

Definition 2.1 ([6, Definition 4.6])**.** A *lifting* of a monad (T, η, μ) on a category C along a fibration $p : \hat{C} \to C$ is a monad $(\hat{T}, \hat{\eta}, \hat{\mu})$ on $\hat{C}$ such that $p \circ \hat{T} = T \circ p$ and $p\hat{\eta} = \eta$ and $p\hat{\mu} = \mu$. If $\hat{C}$ and C are monoidal and T and $\hat{T}$ have strengths σ and $\hat{\sigma}$, then the lifting is *strong* if $p\hat{\sigma} = \sigma$.

Definition 2.2 ([1, Definition 3.3(ii)])**.** Let $(\hat{T}, \hat{\eta}, \hat{\mu})$ be a lifting of (T, η, μ) along a fibration $p : \hat{C} \to C$ equipped with a choice of Cartesian lifts. Given a morphism $f : A \to TB$ in C and an object Q of $\hat{C}$ such that $pQ = TB$, the *weakest precondition of Q on f*, written $\mathrm{wp}_f(Q)$, is the chosen Cartesian lift of Q against f.

We are going to generalize two properties of this framework. The first property is that it can express a standard program logic for the state monad.

Example 2.3 ([1, Remark after Theorem 5.5])**.** Let T be the state monad $TX = S \Rightarrow X \times S$ on **Set** for a fixed set S of states. Let $\mathcal{E}$ be the category whose objects are pairs (X, ϕ) consisting of a set X and a predicate $\phi : X \to \mathbb{P}S$ (equivalently, a subset $\phi : \mathbb{P}(X \times S)$) and whose morphisms $(X, \phi) \to (Y, \psi)$ are functions $f : X \to Y$ such that $\phi(x) \subseteq \psi(f(x))$ for all x in X. The functor $p : \mathcal{E} \to \mathbf{Set}$ that sends (X, ϕ) to X forms a fibration, and the monad T on **Set** lifts along p to the monad $\hat{T}$ given by $\hat{T}(X, \phi) = (TX, \phi')$ where $\phi'(c : TA, s : S) = \phi(c(s))$.

For nontrivial S, this lifting is not strong. If it were strong, ordinary Hoare logic would support a frame rule with respect to conjunction.

The second property we will generalize is that monad liftings are stable under pullback. This allows constructing complex monad liftings from simple pieces.

Theorem 2.4 ([6])**.** *For any monad lifting p of $T : C \to C$ to $\hat{T} : \hat{C} \to \hat{C}$, and any monad morphism $f : T' \to T$, there exists a category $f^*\hat{C}$ and a fibration $f^*p : \hat{C} \to C$ lifting T' to a monad $f^*\hat{T}$ on $\hat{C}$, and this lifting moreover fits into a pullback square of monad liftings.*

Author's Contact Information:

This work aims to develop analogs of these two facts for monad liftings whose associated weakest precondition operates on predicates of separation logic and validates a frame rule.

2.1 Bunched weakest precondition

Definition 2.5. Let $\hat{C}$ be a category that is both Cartesian and symmetric monoidal, and C a Cartesian monoidal category. A *bunched fibration* is a fibration $p : \hat{C} \to C$ such that both the Cartesian and monoidal structures on $\hat{C}$ are sent to the Cartesian structure on C, and such that the functors $\hat{c} \otimes (-) : \hat{C} \to \hat{C}$ preserve Cartesian arrows, for every object $\hat{c} : \hat{C}$.

As validation of this definition, we show that if a bunched fibration is posetal, then it provides a model of the conjunctive fragment of predicate BI.

Proposition 2.6. *Every posetal bunched fibration $p : \hat{C} \to C$ gives rise to a contravariant functor $P : C^{\mathrm{op}} \to \mathbf{CMon}_\wedge$, where $\mathbf{CMon}_\wedge$ is the category of commutative monoids that are also meet-semilattices.*

Our main results are bunched analogs of the two key facts about monad liftings noted above. First, we contribute a definition of *bunched monad lifting*, that generalizes the notion of monad lifting to account for substructural conjunction:

Definition 2.7. A *bunched monad lifting* consists of a bunched fibration $p : \hat{C} \to C$, a monad $\hat{T}$ on $\hat{C}$ equipped with a monoidal strength, and a monad T on C equipped with a Cartesian strength, such that p is a strong monad lifting of T to $\hat{T}$.

Note that $\hat{T}$ has a *monoidal* strength and not a Cartesian one, and that this is the one preserved by p—the Cartesian strength cannot be preserved in general in light of the remarks following Example 2.3. This extra degree of freedom in the definition of bunched monad lifting is what permits a fibrational formulation of weakest precondition for BI. In particular, the monoidal strength gives a fibrational formulation of the frame rule.

As validation of this definition, we show that the standard definition of weakest precondition for separation logic forms a concrete example of a bunched monad lifting:

Proposition 2.8. *Let $H = \mathsf{Loc} \rightharpoonup \mathbb{Z}$ be the set of integer-valued heaps. Let $\mathcal{E}$ be the category whose objects are pairs (A, ϕ) with A a set and $\phi \subseteq A \times H$ a predicate, and whose morphisms (A, ϕ) to (B, ψ) are functions $f : A \to B$ such that $\phi(x, h) \Rightarrow \psi(f(x), h)$. The projection $p : \mathcal{E} \to \mathbf{Set}$ forms a posetal bunched fibration, and the state monad T with state set H admits a bunched monad lifting along p.*

Our second main result provides a bunched analog of Theorem 2.4.

Theorem 2.9. *Bunched monad liftings are stable under pullback.*

These basic results hint at many possible directions for future research. Our immediate goals include a general formulation of computational adequacy and identifying conditions under which the weakest preconditions are compositional with respect to bind. We would also like to generalize to more features both at the level of computation and at the level of logic, like generalizing Proposition 2.8 to local store or coming up with fibrational formulations of more advanced features of separation logic like higher-order quantification and invariants.

References

[1] Alejandro Aguirre and Shin-ya Katsumata. 2020. Weakest preconditions in fibrations. *Electronic Notes in Theoretical Computer Science* 352 (2020), 5–27.

[2] Bodil Biering, Lars Birkedal, and Noah Torp-Smith. 2007. BI-hyperdoctrines, higher-order separation logic, and abstraction. *ACM Transactions on Programming Languages and Systems (TOPLAS)* (2007).

[3] Aleš Bizjak and Lars Birkedal. 2018. On models of higher-order separation logic. *Electronic Notes in Theoretical Computer Science* 336 (2018), 57–78.

[4] Didier Galmiche, Daniel Méry, and David Pym. 2005. The semantics of BI and resource tableaux. *Mathematical Structures in Computer Science* 15, 6 (2005), 1033–1088.

[5] Bart Jacobs. 2014. Dijkstra Monads in Monadic Computation. In *Coalgebraic Methods in Computer Science - 12th IFIP WG 1.3 International Workshop, CMCS 2014, Colocated with ETAPS 2014, Grenoble, France, April 5-6, 2014, Revised Selected Papers (Lecture Notes in Computer Science, Vol. 8446)*, Marcello M. Bonsangue (Ed.). Springer, 135–150. doi:10.1007/978-3-662-44124-4_8

[6] Shin-ya Katsumata. 2005. A semantic formulation of $\top\top$-lifting and logical predicates for computational metalanguage. In *International Workshop on Computer Science Logic*. Springer, 87–102.

[7] Peter W O'Hearn and David J Pym. 1999. The logic of bunched implications. *Bulletin of Symbolic Logic* 5, 2 (1999), 215–244.

[8] David J Pym. 1999. On bunched predicate logic. In *Proceedings. 14th Symposium on Logic in Computer Science (Cat. No. PR00158)*. IEEE, 183–192.

[9] David J Pym. 2002. *The semantics and proof theory of the logic of bunched implications*. Vol. 26. Springer Science & Business Media.

[10] Nikhil Swamy, Joel Weinberger, Cole Schlesinger, Juan Chen, and Benjamin Livshits. 2013. Verifying higher-order programs with the dijkstra monad. In *ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI '13, Seattle, WA, USA, June 16-19, 2013*, Hans-Juergen Boehm and Cormac Flanagan (Eds.). ACM, 387–398. doi:10.1145/2491956.2491978

[11] Wouter Swierstra. 2009. A Hoare Logic for the State Monad. In *Theorem Proving in Higher Order Logics, 22nd International Conference, TPHOLs 2009, Munich, Germany, August 17-20, 2009. Proceedings (Lecture Notes in Computer Science, Vol. 5674)*, Stefan Berghofer, Tobias Nipkow, Christian Urban, and Makarius Wenzel (Eds.). Springer, 440–451. doi:10.1007/978-3-642-03359-9_30