A Relational Separation Logic for Effect Handlers

PAULO EMÍLIO DE VILHENA, Imperial College London, United Kingdom
SIMCHA VAN COLLEM, Radboud University, The Netherlands
INES WRIGHT, Aarhus University, Denmark
ROBBERT KREBBERS, Radboud University, The Netherlands

Effect handlers offer a powerful and relatively simple mechanism for controlling a program's flow of execution. Since their introduction, an impressive array of verification tools for effect handlers has been developed. However, to this day, no framework can express and prove *relational properties* about programs that use effect handlers in languages such as OCaml and Links, where programming features like mutable state and concurrency are readily available. To this end, we introduce *blaze*, the first *relational separation logic* for effect handlers. We build blaze on top of the Iris framework for concurrent separation logic in Rocq, thereby enjoying the rigour of a mechanised theory and all the reasoning properties of a modern fully-fledged concurrent separation logic, such as modular reasoning about stateful concurrent programs and the ability to introduce user-defined ghost state. In addition to familiar reasoning rules, such as the bind rule and the frame rule, blaze offers rules to reason modularly about programs that perform and handle effects. Significantly, when verifying that two programs are related, blaze *does not* require that effects and handlers from one program be in correspondence with effects and handlers from the other. To assess this flexibility, we conduct a number of case studies: most noticeably, we show how different implementations of an asynchronous-programming library using effects are related to *truly concurrent* implementations. As side contributions, we introduce two new, simple, and general reasoning rules for concurrent relational separation logic that are independent of effects: a *logical-fork rule* that allows one to reason about an arbitrary program phrase as if it had been spawned as a thread and a *thread-swap rule* that allows one to reason about how threads are scheduled.

1 Introduction

Effect handlers [43] are a powerful programming abstraction that separates the use of an effect from its implementation, allowing programmers to write effectful code independently of how these effects are implemented. Its programming interface offers the ability to *perform* and to *handle* effects. Performing an effect is similar to raising an exception: execution is suspended and control is transferred to an enclosing pre-installed handler. Handling an effect is also similar to handling an exception with the key difference that, in addition to the effect's payload, the effect handler also has access to a first-class representation of the suspended program, a *continuation*. When invoked, the continuation resumes the suspended program, but, as a first-class value, the continuation can also be discarded or stored in memory to be invoked later.

The ability to suspend and resume programs can be used to implement interesting features such as coroutines [13] and promise-style asynchronous-programming libraries [18]. However, the ability to manipulate continuations is also dangerous. A continuation can capture resources. It may also contain code that must eventually be called to free up these resources. So, if the continuation is discarded, if it becomes unreachable, or if, for some other reason, it is not invoked, then some resources may never be released. Users of effect handlers must also make sure that the operation of performing an effect is always enclosed by a handler, otherwise, like an uncaught exception, an *unhandled effect* would cause a runtime error. For these reasons, effect handlers are widely seen as an advanced programming feature to be used with care.

Authors' Contact Information: Paulo Emílio de Vilhena, p.de-vilhena@imperial.ac.uk, Imperial College London, London, United Kingdom; Simcha Van Collem, simcha.vancollem@ru.nl, Radboud University, Nijmegen, The Netherlands; Ines Wright, ines.w@cs.au.dk, Aarhus University, Aarhus, Denmark; Robbert Krebbers, mail@robbertkrebbers.nl, Radboud University, Nijmegen, The Netherlands.

An impressive range of tools to help programmers to reason about programs with effect handlers and to avoid these programming errors has been introduced. Programming languages such as Koka [36], Links [12, 25] and Effekt [10], for example, have type systems that statically ensure *effect safety*: unhandled effects are statically ruled out. Multiple other type systems with similar guarantees, covering a comprehensive portion of the design space of handlers, can be found in the literature [4–7, 11, 16, 31, 38, 49, 50, 54, 57].

In this paper, we are interested in expressing and verifying *relational properties* of programs with handlers, namely *program refinement* and *program equivalence*. These relational properties have several interesting applications. One could specify a complex but efficient algorithm or data structure in terms of a simple but inefficient counterpart, or express the correctness condition of *linearizability* for concurrent programs using program refinement [20]. Relational reasoning also plays a key role in compiler verification [2, 23].

The study of relational properties of programs with effect handlers is not new. Building on a logic to reason about equality of programs using effects described by an *algebraic theory* [42], Plotkin and Pretnar [44] introduce the notion of correctness of an effect handler as a relational property: the handler implementation must validate the equations of the corresponding algebraic theory. This seminal work has spawned a fertile investigation of relational logics for effect handlers [39, 47].

In prior work, relational reasoning is limited to a strictly functional setting deprived of built-in imperative features. To verify the correctness of a handler implementation that makes use of imperative features such as mutable state, the algebraic approach of Plotkin and Pretnar [44] requires the user to parameterize the correctness statement with an algebraic theory of state. Although denotational models for *ground store* [30] (that is, store where cells can hold integers, pairs, sums, and references to other cells, but not functions or continuations) and for concurrency under similarly restricted forms of state exist, to our knowledge, ground store and, consequently, unrestricted higher-order store still lack an algebraic treatment. This limitation precludes the application of previous relational-reasoning approaches to programming languages like Links and OCaml, which, in addition to user-defined effects and handlers, have ready support for heap-allocated mutable state. The ability to store continuations on the heap is crucial in the effect-handler-based implementations of asynchronous-programming libraries that we study in this paper (§3.1). Moreover, although user-defined effects and handlers offer a modular basis for effectful programming, it is often the case that the handler-based implementation of an effect is obscured by the combination of advanced programming patterns, whereas its handler-free implementation can be derived directly using imperative features. Therefore, from a reasoning perspective, it is desirable to establish a formal statement relating a user-defined effect to its imperative counterpart. For example, can the the operation `perform Fork task`, which performs the user-defined effect `Fork`, be seen as the operation `fork (task())`, which directly spawns a new thread?

To overcome these limitations and address this question, we introduce *blaze*, the first relational logic for a language supporting effect handlers, heap-allocated state, and primitive concurrency and also the first *relational separation logic* for effect handlers. We build blaze on top of the Iris framework [27–29, 32–34] in the Rocq prover [52], thus providing users with the comfort of a proof assistant, the confidence of a mechanised theory, and the expressiveness of Iris, a modern higher-order concurrent separation logic with powerful features such as support for higher-order functions, user-defined ghost state, and invariants.

The blaze logic in a nutshell. The *refinement relation* $e_l \precsim e_r \langle \mathcal{T} \rangle \{R\}$ of blaze informally states that either e_l diverges, or both e_l and e_r terminate with values v_l and v_r that satisfy the postcondition R. The key ingredient is the parameter $\mathcal{T}$, which specifies the *relational theory* under which the

refinement holds. This notion is inspired by Biernacki et al. [5], but, whereas they use pure (step-indexed [1, 3, 19]) logic to express relational theories, we use separation logic [40, 46], and, whereas they reason at the level of a *transparent* logical interpretation of types, we rely on abstract reasoning rules to manipulate an *opaque* notion of refinement. The novelty of blaze therefore *does not* lie in the construction of its model, which follows Biernacki et al. [5], but on the design of reasoning rules that allow the relational verification of handlers at a high level of abstraction hiding any model-specific details from the user of the logic. Moreover, by building this logic on top of separation logic, we are able to express relational properties that involve primitive effects of the language and that are conditional on the ownership of locations in the heap or on Iris-style ghost state.[1]

Using relational theories we can relate user-defined effects to other user-defined effects, or relate user-defined effects to the native imperative features of the language. Concrete examples include:

(1) Relating the *state effect* to the composition of *reader* and *writer effects*.
(2) Relating the *state effect* effect to primitive load and store operations (§2).
(3) Relating a handler-based implementation of *concurrency* to *true concurrency* (§3.1).
(4) Expressing *algebraic laws*, for example that the non-deterministic choice operator (either implemented using a handler that collects a list of results or implemented using concurrency) satisfies monoid laws (§3.2).

Biernacki et al. [5, §4.2] already support (1). We port their result to blaze as part of our Rocq formalisation [17]. More crucially, by using separation logic to formulate our relational theories, blaze also supports (2) and (3). Another application of blaze is (4), which enables the formulation of a handler-correctness criterion in the style of Plotkin and Pretnar [44]. Expressing handler correctness in this style is novel in the context of higher-order state and primitive concurrency. However, unlike Plotkin and Pretnar [44]'s algebraic theories, we note that algebraic theories expressed in blaze are not transitive due to a known limitation of step-indexed relational logics [8, 26].

We give a semantics to the refinement relation $e_l \precsim e_r \langle \mathcal{T} \rangle \{R\}$ using an interpretation in Iris. At the basis, we use Iris's weakest precondition assertion to define *observational refinement* in the same way as ReLoC [22, §7.1]. Then, taking inspiration from Pitts and Stark [41]'s *biorthogonality* technique (used for the first time by Biernacki et al. [5] in the context of effect handlers) we define refinement, mutually inductively with two other relations, using Iris's guarded fixpoint operator.

While this layering of definitions makes it possible to bootstrap blaze, it also makes it infeasible to carry out refinement proofs directly by unfolding these definitions, let alone carry out these proofs in a compositional manner. We therefore take inspiration from ReLoC [21, 22] and Simuliris [2, 23] to develop a *relational logic* with a range of high-level reasoning principles that abstract over the details of these definitions. Our high-level logic provides a number of novel features:

(1) Our novel *introduction* and *exhaustion rules* make it possible to abstractly manipulate a relational theory $\mathcal{T}$. If $\mathcal{T}$ contains a relation between e_l and e_r, then the introduction rule allows us to prove $e_l \precsim e_r \langle \mathcal{T} \rangle \{R\}$. The exhaustion rule allows us to eliminate the dependency on a theory $\mathcal{T}$, provided that the relations included in $\mathcal{T}$ are correctly handled.
(2) The *bind rule* makes it possible to focus on a subexpression and then continue with the verification of the whole expression in which the subexpression is replaced with a value. It is well known that, in the context of logics for effect handlers, a restriction on the bind rule is necessary for soundness. We develop a new restriction that requires the bound contexts to be *traversable* with respect to the relational theory $\mathcal{T}$. This flexibility is crucial to support dynamic effects labels.

[1] Adding support for primitive effects, particularly concurrency, in a relational separation logic is not as straightforward as it may sound. Our proof rules for state directly follow ReLoC [22]. However, as we discuss in §3.1.1, such an approach does not go as smoothly for concurrency. We instead design original rules for reasoning about concurrency.

We show the versatility of our approach through various extensions. We add support for dynamic labels in the style of OCaml's **let exception** construct, following de Vilhena and Pottier [16]. Moreover, we add support for both one-shot and multi-shot continuations, taking inspiration from van Rooij and Krebbers [54]. Finally, as a side contribution needed to carry out some of our case studies, we introduce new relational rules for concurrency. These rules are independent of effect handlers and hold in any Iris-style relational logic such as ReLoC [21, 22].

Contributions. In sum, our contributions are the following:

(1) **Novel relational logic.** We introduce blaze, the first relational separation logic for handlers.
(2) **Case studies.** We conduct several challenging case studies including the verification that multiple effect-handler-based implementations of concurrency refine *truly concurrent* ones.
(3) **Novel reasoning rules.** Our case studies led us to discover novel, simple, and general reasoning rules in relational concurrent separation logic that are independent of handlers.
(4) **Correctness with respect to algebraic theories.** We show how the correctness of an effect handler with respect to an algebraic theory can be stated and proved in blaze.
(5) **Mechanised theory.** We mechanise all our results, including soundness, in the Rocq prover.

2 Overview

In this section, we discuss the main challenges in designing a relational separation logic with support for effect handlers. Our goal is to informally explain how blaze handles these challenges. The examples are written in λ-blaze, a calculus whose syntax and semantics we explain in **??**. In this section, we assume familiarity with functional programming and effect handlers. For the unaccustomed reader, Pretnar [45] provides a tutorial introduction to effect handlers.

Let us start by considering the following example:

```
countdown ≜ fun timer.
  timer.set 10; while (timer.get() > 0) {timer.set (timer.get() - 1)}
```

The function *countdown* receives an object *timer* as an argument with two fields, `get` and `set`. It assumes these fields implement the functionality to respectively access and update *timer*'s memory. It uses this functionality to update the timer from `10` to `0` through decrements of `1`.

The definition of *countdown* is modular on the implementation of the timer. In a language with effect handlers, the programmer can exploit this generality by implementing `get` and `set` as user-defined effects and providing different handlers to customise the implementation of the effects performed by `get` and `set`. For example, assuming an effect `$Timer` is available, a generic implementation of `get` and `set` can be obtained as follows:

```
timer ≜ {get = fun _. perform $Timer (inl ()); set = fun y. perform $Timer (inr y)}
```

The operations `get` and `set` perform the effect `$Timer`. The *left and right injections* **inl** and **inr** are used to distinguish requests sent by `get` and `set`. A `$Timer` handler eventually assigns meaning to `get` and `set` by replying to these requests. Here are two possible instances of such handlers:

```
run_st_passing ≜ fun main.
  let run = fun ().
    handle main() with
    | effect $Timer request, k ⇒ fun x.
        match request with
        | inl () ⇒ k x x
        | inr y ⇒ k () y
    | y ⇒ fun _. y
  in run() 0
```

```
run_heap ≜ fun main.
  let r = ref 0 in
  handle main() with
  | effect $Timer request, k ⇒
      match request with
      | inl () ⇒ k (!r)
      | inr y ⇒ r ← y; k ()
  | y ⇒ y
```

Both receive a piece of client code *main* that performs `$Timer` effects. The function *run_st_passing* installs a handler that interprets `$Timer` effects in *state-passing style*, whereby the computation is transformed into a function that takes the current state of the timer and outputs the timer's final state. In contrast, the function *run_heap* interprets `$Timer` effects by storing the current state of the timer in a local reference r. This implementation is arguably simpler than the state-passing implementation of *run_st_passing* although presumably they implement the same functionality.

This observation motivates a key question: is it possible to show that *run_st_passing* is a *refinement* of *run_heap*? That is, can *run_heap* be used as a *specification* of *run_st_passing* and, therefore, as a *reference implementation* of `get` and `set`?

The notion of refinement is formalised in relational logics as the relation $e_l \precsim e_r \{R\}$, where e_l and e_r are expressions and the *postcondition* R is a relation on values. We refer to e_l as the expression on the *implementation side* and to e_r as the expression on the *specification side*. The refinement relation informally states that either e_l diverges or both e_l and e_r terminate with outputs v_l and v_r such that $R(v_l,\ v_r)$ holds, capturing the intuition that e_l implements the same functionality described by e_r, because, informally, every output of e_l corresponds to an output of e_r related by R.

The question can thus be reformulated as how to establish a refinement between *run_st_passing* and *run_heap*, such as the statement

$$\mathit{impl}_1 \precsim \mathit{impl}_2\ \{y_l\ y_r.\ y_l = y_r\},\quad \begin{array}{rl} \text{where } \mathit{impl}_1 & \triangleq\ \mathit{run\_st\_passing}\ (\mathbf{fun}\ ().\ \mathit{countdown\ timer}) \\ \text{and } \mathit{impl}_2 & \triangleq\ \mathit{run\_heap}\ (\mathbf{fun}\ ().\ \mathit{countdown\ timer}), \end{array} \tag{1}$$

expressing the property that impl_1 and impl_2 have the same outputs.

To our knowledge, there are no relational logics with support for effect handlers *and* heap-allocated mutable state and therefore no logics where such a relation can be derived. Addressing this gap, we introduce blaze, the first relational separation logic with support for handlers. The choice of a separation logic enables modular reasoning about state-manipulating programs such as *run_heap*. The following subsections explain other interesting and novel aspects of blaze.

2.1 Modular reasoning about effects: handler versus handlee

In blaze, it is possible to state and prove Refinement 1. In fact, this refinement can be established in a *compositional* way, whereby the proof is split into two parts: a proof that the handlers installed by *run_st_passing* and *run_heap* are related and a proof that the handlees monitored by these handlers are related. In the current example, this creates the following two subgoals:

$$\mathit{countdown\ timer} \overset{?}{\precsim} \mathit{countdown\ timer} \tag{2}$$

$$\forall \mathit{main}_l,\ \mathit{main}_r.\ \mathit{main}_l\,() \overset{?}{\precsim} \mathit{main}_r\,() \mathrel{-\!\!*} \mathit{run\_st\_passing}\ \mathit{main}_l \precsim \mathit{run\_heap}\ \mathit{main}_r\ \{=\} \tag{3}$$

Refinement 2 relates the handlees and Refinement 3 relates *run_st_passing* and *run_heap* under the assumption they receive related arguments. For brevity, we write "=" in Refinement 3 for the postcondition $y_l\ y_r.\ y_l = y_r$. Moreover, we use $\overset{?}{\precsim}$ to denote a notion of refinement that is yet to be defined. Recall that the informal reading of $\mathit{countdown\ timer} \precsim \_\ \{\_\}$ states *countdown timer* either diverges or terminates with a value. This standard notion of refinement $\_ \precsim \_\ \{\_\}$ is therefore insufficient, because, without a handler, the program *countdown timer* performs unhandled effects.

This limitation reveals a *key challenge*: to reason about the handlee independently of the handler, it is necessary to generalise the standard notion of refinement to account for unhandled effects.

The blaze logic solves this challenge by parameterising the refinement relation with a *relational theory*. A relational theory can be seen as a set of assumed refinements. Concretely, it is defined as a set of triples $(e_l,\ e_r,\ Q)$, where e_l and e_r are expressions and Q is a relation on pairs of expressions called the *return condition*. In short, the return condition describes the condition under which e_l and e_r can return. For example, the return condition $y_l\ y_r.\ y_l = y_r$ states e_l and e_r can return only

when they terminate with the same values. In this case, the return condition Q can be seen as a postcondition. The reading of $(e_l,\ e_r,\ Q)$ then simply states that e_l refines e_r with postcondition Q. For the purposes of this section, this first approximation is enough.

The general refinement relation in blaze has the form $e_l \precsim e_r\ \langle \mathcal{T} \rangle\ \{R\}$, where $\mathcal{T}$ is the parameterised relational theory. When a relational theory is empty, we write $e_l \precsim e_r\ \{R\}$ which has the same informal meaning as before. The informal reading of the general relation $e_l \precsim e_r\ \langle \mathcal{T} \rangle\ \{R\}$ is that $K_l[e_l] \precsim K_r[e_r]\ \{R\}$ holds for every pair of contexts K_l and K_r that *validate the theory* $\mathcal{T}$. A pair of contexts K_l and K_r validate $\mathcal{T}$ when the refinements included in $\mathcal{T}$ hold under K_l and K_r; that is, if $\mathcal{T}$ includes the relation between two expressions e_l and e_r, then $K_l[e_l]$ refines $K_r[e_r]$. This general notion of refinement allows us to reason about programs e_l and e_r that perform unhandled effects, because, when $\mathcal{T}$ is well-chosen, the contexts K_l and K_r that validate $\mathcal{T}$ are precisely those that handle the effects performed by e_l and e_r. At the same time, the contexts K_l and K_r appear only in the definition of $e_l \precsim e_r\ \langle \mathcal{T} \rangle\ \{R\}$, which, during a verification task, need not be unfolded. The theory $\mathcal{T}$ can thus be seen as a logical abstraction of the contexts under which e_l and e_r occur.

In the running example of Refinements 2 and 3, it is now possible to substitute $\overset{?}{\precsim}$ with a refinement relation parameterised by a relational theory, say $\mathit{Timer}_{\mathit{refl}}$:

$$\_ \overset{?}{\precsim} \_ \quad \triangleq \quad \_ \precsim \_\ \langle \mathit{Timer}_{\mathit{refl}} \rangle\ \{=\}$$

There are two minimal requirements for the relational theory $\mathit{Timer}_{\mathit{refl}}$: (1) $\mathit{Timer}_{\mathit{refl}}$ must include sufficiently many relations so that $\mathit{countdown\ timer} \precsim \mathit{countdown\ timer}\ \langle \mathit{Timer}_{\mathit{refl}} \rangle\ \{=\}$ holds and (2) $\mathit{Timer}_{\mathit{refl}}$ must be sufficiently small so that $\mathit{run\_st\_passing}\ \mathit{main}_l \precsim \mathit{run\_heap}\ \mathit{main}_r\ \{=\}$ holds under the assumption that $\mathit{main}_l\,() \precsim \mathit{main}_r\,()\ \langle \mathit{Timer}_{\mathit{refl}} \rangle\ \{=\}$ holds. A choice of $\mathit{Timer}_{\mathit{refl}}$ that satisfies both requirements is one that includes only the following refinement:

$$\forall v.\ \texttt{perform}\ \texttt{\$Timer}\ v \precsim \texttt{perform}\ \texttt{\$Timer}\ v\ \langle \mathit{Timer}_{\mathit{refl}} \rangle\ \{=\} \tag{4}$$

This is sufficient to prove $\mathit{countdown\ timer} \precsim \mathit{countdown\ timer}\ \langle \mathit{Timer}_{\mathit{refl}} \rangle\ \{=\}$, because, as the two expressions in this relation are same, every `$Timer` effect on one side corresponds to exactly one `$Timer` effect on the other side. Therefore, when reasoning about performing an effect, it suffices to apply Refinement 4 to conclude that, in both expressions, the results are the same.

Moreover, because $\mathit{Timer}_{\mathit{refl}}$ includes only Refinement 4, it follows that, if $e_l \precsim e_r\ \langle \mathit{Timer}_{\mathit{refl}} \rangle\ \{=\}$ holds for arbitrary expressions e_l and e_r, then it must be the case that every `$Timer` effect in e_l corresponds to exactly one `$Timer` effect in e_r. This assumption can be exploited by the proof of $\mathit{run\_st\_passing}\ \mathit{main}_l \precsim \mathit{run\_heap}\ \mathit{main}_r\ \{=\}$ to establish the relation between the two handlers.

2.2 Flexible reasoning: handler-based versus handler-free implementations

One of the motivations to establish the refinement between *run_st_passing* and *run_heap* is that *run_heap* provides a simpler and more direct implementation of the timer when compared to the state-passing implementation of *run_st_passing*. However, *run_heap* does not exploit non-trivial functionalities of effect handlers as the effect branch always immediately resumes the continuation. This observation permits an implementation of the timer without effects:

$$\mathit{ref\_timer} \ \triangleq\ \texttt{fun}\ r.\ \{\texttt{get} = \texttt{fun}\ ().\ !r;\ \texttt{set} = \texttt{fun}\ y.\ r \leftarrow y\}$$

The question now is: can the refinement

$$\mathit{impl}_1 \precsim \mathit{impl}_3\ \{=\},\ \text{where}\ \mathit{impl}_3\ \triangleq\ \texttt{let}\ r = \texttt{ref}\ 0\ \texttt{in}\ \mathit{countdown}\ (\mathit{ref\_timer}\ r), \tag{5}$$

be established in blaze? Moreover, if possible, can the proof be done in a compositional way like in the previous example, where reasoning about handlee and handler are carried out independently?

The answers to both questions are positive: the refinement can be established in blaze with a compositional proof. Indeed, the proof of $\mathit{impl}_1 \lesssim \mathit{impl}_3\ \{=\}$ is split into two subgoals:

$$\forall \ell.\ \ell \overset{1/2}{\mapsto}_{\mathtt{s}} \mathtt{0} \mathrel{-\!\!*} \mathit{countdown\ timer} \lesssim \mathit{countdown}\ (\mathit{ref\_timer}\ \ell)\ \langle \mathit{Timer}^{\ell}_{\mathit{spec}} \rangle\ \{=\} \tag{6}$$

$$\forall \ell,\ \mathit{main}_l,\ e_r.\ \ell \overset{1/2}{\mapsto}_{\mathtt{s}} \mathtt{0} \mathrel{-\!\!*} \mathit{main}_l\,() \lesssim e_r\ \langle \mathit{Timer}^{\ell}_{\mathit{spec}} \rangle\ \{=\} \mathrel{-\!\!*} \mathit{run\_st\_passing}\ \mathit{main}_l \lesssim e_r\ \{=\} \tag{7}$$

Refinement 6 relates the handlee *countdown timer* to *countdown* (*ref_timer* ℓ) under the theory $\mathit{Timer}^{\ell}_{\mathit{spec}}$, which we introduce shortly. Refinement 7 is stated in an interesting way. It relates *run_st_passing* main_l to an arbitrary expression e_r. Intuitively, the expression represents the program *countdown* (*ref_timer* ℓ), but, thanks to the theory $\mathit{Timer}^{\ell}_{\mathit{spec}}$, this specific program can be entirely abstracted: all the information needed to carry out Refinement 7 is that main_l refines e_r under $\mathit{Timer}^{\ell}_{\mathit{spec}}$.

The variable ℓ stands for the location to which r (in impl_3) is bound. As usual in relational separation logics, each of the two programs in a refinement relation manipulates its own heap. The *points-to predicate* $\_ \mapsto_{\mathtt{s}} \_$ describes the state of the heap of the program on the specification side, whereas $\_ \mapsto_{\mathtt{i}} \_$ describes the state of the heap on the implementation side. The fraction that appears on top of $\mapsto_{\mathtt{s}}$ represents a *fractional ownership* [9] of ℓ: it grants read-only permission to ℓ. Full ownership can be retrieved by combining two $\ell \overset{1/2}{\mapsto}_{\mathtt{s}} \_$ assertions. In the proof of Refinement 5, fractional assertions $\ell \overset{1/2}{\mapsto}_{\mathtt{s}} \_$ are given to both the handlee and the handler. Full ownership is therefore retrieved when the handlee performs an effect and ownership of the handlee's fractional assertion $\ell \overset{1/2}{\mapsto}_{\mathtt{s}} \_$ is temporarily transferred to the handler until the handlee is resumed.

Like $\mathit{Timer}_{\mathit{refl}}$, the theory $\mathit{Timer}^{\ell}_{\mathit{spec}}$ must fulfil two requirements: (1) the theory must be sufficiently relaxed so that Refinement 6 can be established and (2) it must be sufficiently small so that the terms $\mathit{main}_l()$ and e_r in Refinement 7 are tightly related. The first requirement now seems particularly challenging because Refinement 6 relates an effectful program to a non-effectful one. Fortunately, relational theories are not limited to relations between only effectful expressions like in $\mathit{Timer}_{\mathit{refl}}$. They can in fact express relations between arbitrary expressions. Taking advantage of this flexibility, the theory $\mathit{Timer}^{\ell}_{\mathit{spec}}$ includes a relation between the effectful implementation of `get` and `set` fields of *timer* and their heap-manipulating counterparts of *ref_timer*:

$$\forall x.\ \ell \overset{1/2}{\mapsto}_{\mathtt{s}} x \mathrel{-\!\!*} \mathtt{perform}\ \mathtt{\$Timer}\ (\mathtt{inl}\ ())) \lesssim !\ell\ \langle \mathit{Timer}^{\ell}_{\mathit{spec}} \rangle\ \{y_l\ y_r.\ y_l = y_r = x\ *\ \ell \overset{1/2}{\mapsto}_{\mathtt{s}} x\} \tag{8}$$

$$\forall y.\ \ell \overset{1/2}{\mapsto}_{\mathtt{s}} \_ \mathrel{-\!\!*} \mathtt{perform}\ \mathtt{\$Timer}\ (\mathtt{inr}\ y) \lesssim \ell \leftarrow y\ \langle \mathit{Timer}^{\ell}_{\mathit{spec}} \rangle\ \{y_l\ y_r.\ y_l = y_r = ()\ *\ \ell \overset{1/2}{\mapsto}_{\mathtt{s}} y\} \tag{9}$$

From the perspective of the handlee, these relations guarantee that performing the effect `$Timer` is similar to manipulating the memory location ℓ.

2.3 Context-local relational reasoning

A closer look at Refinements 8 and 9 reveals an important limitation. They apply only to pairs of programs e_l and e_r where e_l consists precisely of a single `$Timer` effect and e_r consists precisely of a single read or store operation. As such, they are insufficient to establish Refinement 6, because the calls to `get` and `set` in *countdown timer* and in *countdown* (*ref_timer* ℓ) occur in the context of a larger program, not as single operations.

The key missing principle to address this limitation is the *bind rule*. The bind rule allows the user to reason about a piece of code independently of the context under which this code is eventually executed. In standard relational logics, the bind rule is formally stated as follows:

$$\textsc{standard-bind} \quad e_l \lesssim e_r\ \{y_l\ y_r.\ K_l[y_l] \lesssim K_r[y_r]\ \{R\}\} \vdash K_l[e_l] \lesssim K_r[e_r]\ \{R\}$$

This rule is sound in blaze, but insufficient because it assumes the parameterised theory is empty. A natural fix would be to decorate every occurrence of the refinement relation with a theory $\mathcal{T}$:

$$\textsc{unsound-bind} \quad \cancel{e_l \lesssim e_r \langle \mathcal{T} \rangle \{y_l\, y_r.\ K_l[y_l] \lesssim K_r[y_r] \langle \mathcal{T} \rangle \{R\}\} \vdash K_l[e_l] \lesssim K_r[e_r] \langle \mathcal{T} \rangle \{R\}}$$

The resulting rule is *unsound*. To see why, it suffices to consider the following counterexample, where the effect `$Id` is assumed to be available:

$$e_{true} \triangleq \texttt{handle (perform \$Id true) with effect \$Id } x\texttt{, } k \Rightarrow k\, x \texttt{ | } y \Rightarrow y$$

If we further assume there is a theory *Neq* that includes the refinement $\forall b \in \mathit{Bool}.$ `perform $Id` $b \lesssim$ `perform $Id` $b \langle \mathit{Neq} \rangle \{\neq\}$, then, using UNSOUND-BIND with both K_l and K_r instantiated as the `$Id` handler, it is possible to establish the refinement $e_{true} \lesssim e_{true} \langle \mathit{Neq} \rangle \{\neq\}$, which is false, because both sides of the refinement terminate with `true`.

This counterexample suggests that to enable sound context-local reasoning, there must be some restriction on the evaluation contexts K_l and K_r. In particular, the rule should not be applicable when the contexts K_l and K_r contain handlers for the effects described by the theory $\mathcal{T}$. In blaze, a sound bind rule integrating these restrictions is formulated as follows:

$$\textsc{bind} \quad \frac{\mathit{traversable}(K_l,\, K_r,\, \mathcal{T}) \qquad \mathcal{T} \sqsubseteq \mathcal{F} \\ e_l \lesssim e_r \langle \mathcal{T} \rangle \{y_l\, y_r.\ K_l[y_l] \lesssim K_r[y_r] \langle \mathcal{F} \rangle \{R\}\}}{\vdash K_l[e_l] \lesssim K_r[e_r] \langle \mathcal{F} \rangle \{R\}}$$

The rule is applicable when there exists a theory $\mathcal{T}$ *included* in $\mathcal{F}$, such that $\mathit{traversable}(K_l,\, K_r,\, \mathcal{T})$ holds. The predicate $\mathit{traversable}(K_l,\, K_r,\, \mathcal{T})$ intuitively states that K_l and K_r do not conflict with $\mathcal{T}$, or, visually, that $\mathcal{T}$ can *traverse* K_l and K_r. It is defined in an abstract way with no reference to the handlers in K_l and K_r. In the case of $\mathit{Timer}_{\mathit{refl}}$, it is possible to show this predicate holds for any contexts K_l and K_r that contain no `$Timer` handler. In the case of $\mathit{Timer}^{\ell}_{\mathit{spec}}$, the predicate holds for any K_l that contains no `$Timer` handler. No condition is imposed on K_r in this case, because the expressions on the right-hand side of Refinements 8 and 9 do not perform effects. The blaze logic therefore enjoys a powerful context-local reasoning principle that is adjustable to the parameterised theory. As we are going to show in **??**, this principle is especially important to support reasoning in the presence of multiple effect names.

3 Case Studies

To assess the usability of our logic, we verify refinement statements for a number of interesting effects including *concurrency* (§3.1), *Haskell-like non-determinism* (§3.2), and *state*, where, like Biernacki et al. [5, §4.2], we show state can be implemented in terms of two independent *reader* and *writer* effects. In the interest of space, we do not discuss this state effect in detail. Its implementation can be found in the Appendix (§C.1). Mechanised proofs of all case studies are included in our Rocq formalisation [17].

3.1 Concurrency

Effect handlers enable the implementation of *cooperative-concurrency* libraries. In such libraries, multiple tasks can be spawned and their execution is monitored by a scheduler making sure at most one task runs at a time. It is an important and interesting application of effect handlers, serving as the "*primary motivation*" for the addition of effect handlers to OCaml [37, §24.5]. Here is the handler-based implementation of a *fork effect* [7, Fig. 11] in λ-blaze:

```
run_fork ≜ fun main.
  let effect Fork in let q = new_queue() in
  let run = rec run task. handle task() with
    | effect Fork task', k ⇒ push q k; run task'
    | _ ⇒ if empty q then () else (let k = pop q in k())
  in run (fun _. main (fun task'. perform Fork task'))
```

$$\mathit{runForkSpec} \triangleq \Box \forall\, \mathit{main}_1,\ \mathit{main}_2.\ \left(\begin{array}{l}\forall \mathit{fork}_1,\ \mathit{fork}_2,\ \mathcal{L}.\\ \mathit{forkSpec}(\mathit{fork}_1,\ \mathit{fork}_2,\ \mathcal{L}) \mathrel{-\!\!*}\\ \mathit{main}_1\ \mathit{fork}_1 \precsim_\star \mathit{main}_2\ \mathit{fork}_2\ \langle \mathcal{L} \rangle\ \{\mathsf{True}\}\end{array}\right) \mathrel{-\!\!*} \begin{array}{l}\mathit{run\_fork}\ \mathit{main}_1 \precsim_\star\\ \mathit{main}_2\ (\mathbf{fun}\ \mathit{task}'.\ \mathbf{fork}\ (\mathit{task}'()))\ \{\mathsf{True}\}\end{array}$$

$$\mathit{forkSpec}(\mathit{fork}_1,\ \mathit{fork}_2,\ \mathcal{L}) \triangleq \Box \forall \mathit{task}_1,\ \mathit{task}_2.\ \mathit{task}_1()\precsim_\star \mathit{task}_2()\ \langle \mathcal{L} \rangle\ \{\mathsf{True}\} \mathrel{-\!\!*} \mathit{fork}_1\ \mathit{task}_1 \precsim_\star \mathit{fork}_2\ \mathit{task}_2\ \langle \mathcal{L} \rangle\ \{\mathsf{True}\}$$

Fig. 1. Fork case study: Specification.

The function *run_fork* supplies a piece of client code *main* with the functionality to fork tasks by monitoring the execution of *main* with a handler for the `Fork` effect. The handling of a `Fork` effect with payload task' pushes the paused continuation k to a queue q. This queue is allocated at the beginning of *run_fork*'s execution. It is initially empty, and, as an invariant, it stores continuations that can be readily resumed with `()`. Updates to q maintain this invariant, because, thanks to a deep-handler semantics, the continuation k includes the `Fork` handler at its top-most frame. After this update, the handling of `Fork` terminates by running task' under a new `Fork` handler. When a task terminates, if the handler finds q non-empty, it pops a continuation k from q representing a previously paused task and resumes the execution of this task. If q is empty then all scheduled tasks have executed, so the function *run_fork* terminates.

The implementation of *run_fork* is concise, but relies on advanced programming features, notably, the ability to reify contexts as first-class continuations using handlers and the ability to place these continuations in the store. The complexity of *run_fork*'s operational behaviour motivates the question: is it possible to show that the fork functionality implemented by *run_fork* can be abstracted as a real concurrent fork instruction?

In this case study, we answer this question positively by verifying in blaze that the functionality implemented by *run_fork* refines the primitive **fork** construct of λ-blaze. The formal statement is written in Figure 1. The specification of *run_fork*, the assertion *runForkSpec*, states a refinement between the application of *run_fork* to a client main_1 and the application of a client main_2 to a function $\mathbf{fun}\ \mathit{task}'.\ \mathbf{fork}\ (\mathit{task}'())$ that directly forks task'. The clients main_1 and main_2 are universally quantified in this specification. It is assumed that main_1 and main_2 can be related when respectively supplied with abstract fork implementations fork_1 and fork_2. It is the obligation of the user of the library to show the relation between $\mathit{main}_1\ \mathit{fork}_1$ and $\mathit{main}_2\ \mathit{fork}_2$. To establish this relation, the user can rely on a relational specification of fork_1 and fork_2, the assertion *forkSpec*, stating a relation between the application of fork_1 to a task task_1 and the application of fork_2 to a task task_2. To use this specification, it is again an obligation of the user to establish the relation between $\mathit{task}_1()$ and $\mathit{task}_2()$. In establishing this relation, the user can still rely on *forkSpec* to relate further calls to fork_1 and fork_2 in the tasks task_1 and task_2. The refinement between main_1 and main_2 is carried out under an abstract theory list $\mathcal{L}$. Intuitively, this list represents the internal relational theory that is used by *run_fork* to relate `Fork` to **fork**. Apart from $\mathcal{L}$, which is abstract to the user, the specification *runForkSpec* assumes an *empty* ambient theory to relate the effects of main_1 and main_2 as well as the effects of two forked tasks task_1 and task_2. In other words, the specification disallows main_1 and main_2 as well as forked tasks to perform unhandled effects. This limitation is necessary because forked tasks on the specification side of the refinement run on new empty contexts, where performing an unhandled effect constitutes a runtime error.

$$\textsc{fork-l-}\star\ \frac{i \Mapsto e_r \qquad e_l \precsim_\star e_r\ \langle \mathcal{L}^\perp \rangle\ \{\mathsf{True}\} \qquad K_l[\,()\,] \precsim_\star e_r'\ \langle \mathcal{L} \rangle\ \{R\}}{K_l[\mathbf{fork}\ e_l] \precsim_\star e_r'\ \langle \mathcal{L} \rangle\ \{R\}} \qquad \textsc{fork-r-}\star\ \frac{\forall i.\ i \Mapsto e_r \mathrel{-\!\!*} e_l \precsim_\star K_l[\,()\,]\ \langle \mathcal{L} \rangle\ \{R\}}{e_l \precsim_\star K_l[\mathbf{fork}\ e_r]\ \langle \mathcal{L} \rangle\ \{R\}}$$

$$\textsc{logical-fork-}\star\ \frac{i \Mapsto K_r[e_r] \qquad e_l \precsim_\star e_r\ \langle \mathcal{L}^\perp \rangle\ \{R\} \qquad \forall v_l, v_r.\ R(v_l, v_r) \mathrel{-\!\!*} i \Mapsto K_r[v_r] \mathrel{-\!\!*} K_l[v_l] \precsim_\star e_r'\ \langle \mathcal{L} \rangle\ \{S\}}{K_l[e_l] \precsim_\star e_r'\ \langle \mathcal{L} \rangle\ \{S\}}$$

$$\textsc{thread-swap-}\star\ \frac{i \Mapsto K[e_r] \qquad \forall j, K'.\ j \Mapsto K'[e_r'] \mathrel{-\!\!*} e_l \precsim_\star e_r\ \langle \mathcal{L}^\perp \rangle\ \{v_l\ \_.\ \exists v_r'.\ j \Mapsto K'[v_r'] \ *\ R(v_l, v_r')\}}{e_l \precsim_\star e_r'\ \langle \mathcal{L} \rangle\ \{R\}}$$

Fig. 2. Reasoning rules for concurrency.

3.1.1 Relational reasoning about concurrency. Before presenting the proof of *runForkSpec*, we explain how we extend blaze with support for reasoning about native concurrency.[2] The logic has support for invariants in the same way as ReLoC [22]: there are two general rules for allocating and closing invariants and one invariant-opening rule per atomic instruction. In the interest of space, we do not discuss these rules, because they are not needed in our case studies.[3] Invariants are not needed, because, in all case studies, native concurrency occurs only on the specification side of the refinement, whereby, thanks to an *angelic* flavour of non-determinism, the user is (or should be) capable of deciding how threads interleave to avoid interference. Despite the substantial literature on relational concurrent separation logic [21, 22, 55, 56], we found that rules to achieve such a desirable reasoning ability are lacking with respect to three key limitations which we explain next. To address these limitations, we design *novel* relational reasoning rules for concurrency.

Limitation to refinements where **fork***s match.* In previous work (for example [22, §4.1]), it is assumed that **fork** instructions on both sides of a refinement match. This is clearly not the case for the refinement *runForkSpec* because only the specification side forks threads directly. To overcome this limitation, we follow Vindum et al. [56] in exposing the ghost thread-pool assertion $i \Mapsto e$[4] in the logic. Recall that its reading simply states thread i at the specification side runs e. Using this resource, we can split a traditional relational *fork rule* into Rules FORK-L-$\star$ and FORK-R-$\star$, shown in Figure 2. Rule FORK-R-$\star$ forges a new resource $i \Mapsto e_r$. There are many ways to spend this resource. Rule FORK-L-$\star$ consumes it to allow reasoning about a **fork** e_l instruction on the implementation side. As a condition to this rule, the expressions e_l and e_r must be related under the theory list $\mathcal{L}^\perp$, which sets every theory in $\mathcal{L}$ to $\perp$. This condition guarantees the forked threads do not perform unhandled effects.

Explicit operational reasoning about thread-pool assertions. The reasoning rules introduced by Vindum et al. [56, Fig. 8] require the user to explicitly manipulate thread-pool resources; that is, the user must inspect the shape of the expression e_r in an assertion $i \Mapsto e_r$ and select one of their rules allowing e_r to be partially executed. This is a strong limitation for the verification of *runForkSpec*, because the only assumption on forked tasks $task_1$ and $task_2$ is that $task_1()$ refines $task_2()$. The specific shape of $task_2$ is unknown. To overcome this limitation, we introduce

[2]We focus on blaze but similar reasoning principles can be achieved in baze (Figure 12).
[3]The rules for allocating, opening, and closing invariants can be found in the Appendix (§C.4).
[4]Vindum et al. [56] in fact present this resource as a *right refinement*. In our logic, the user does not explicitly manipulate this resource; it is already abstract as is, so we can keep its standard notation.

Relational theory.

$$\begin{aligned} &\mathit{Fork}(\textbf{perform}\ \$\mathtt{Fork}\ \mathit{task}_1,\ \textbf{fork}\ (\mathit{task}_2\,()),\ Q) \triangleq \\ &\quad \triangleright\, \mathit{task}_1\,() \precsim_\star \mathit{task}_2\,()\ \langle [([\$\mathtt{Fork}],\ [],\ \mathit{Fork})] \rangle\ \{\mathsf{True}\} \ast Q((),\ ()) \end{aligned}$$

Invariants and predicates.

$$\begin{aligned} &\mathit{queueInv}(q,\ \mathit{ks},\ \mathit{ks}') \triangleq \mathit{isQueue}(q,\ \mathit{ks}.1) \ast \\ &\quad \left(\ast_{(k,\,(j,\,K))\in \mathit{ks}} \cdot\ \exists e_r.\ j \Rrightarrow K[e_r] \ast \mathit{ready}(q,\ k\,(),\ e_r)\right) \ast \left(\ast_{(\_,\,(j,\,K))\in \mathit{ks}'} \cdot\ \exists v_r.\ j \Rrightarrow K[v_r]\right) \\ &\mathit{ready}(q,\ e_l,\ e_r) \triangleq \forall \mathit{ks},\ \mathit{ks}'.\ \triangleright\, \mathit{queueInv}(q,\ \mathit{ks},\ \mathit{ks}') \mathrel{-\!\!*} \\ &\quad e_l \precsim_\star e_r\ \langle [([\$\mathtt{Fork}],\ [],\ \bot)] \rangle\ \{\mathit{queueInv}(q,\ [],\ \mathit{ks} +\!\!+ \mathit{ks}')\} \end{aligned}$$

Fig. 3. Fork case study: Internal logical definitions.

Rule LOGICAL-FORK-★ (Figure 2). This rule consumes a thread-pool resource $i \Rrightarrow K_r[e_r]$ and, as a condition, the user must supply a subexpression e_l that refines e_r. In return, the user can reclaim the assertion $i \Rrightarrow K_r[v_r]$ where e_r is replaced with its result v_r, obtained with no explicit manipulation of the thread-pool assertion. This rule can be used in conjunction with Rule FORK-R-★ to derive the refinement $e_1 \precsim e_1'\ \{\mathsf{True}\} \mathrel{-\!\!*} e_2 \precsim e_2'\ \{\mathsf{True}\} \mathrel{-\!\!*} e_1\,;\, e_2 \precsim \textbf{fork}\ (e_1')\,;\, e_2'\ \{\mathsf{True}\}$, which cannot be shown using the rules in Vindum et al. [56, Fig. 8] without breaking the abstraction of their refinement relation.

Access to thread-pool resource describing the main thread. With the rules discussed so far, the only way to obtain new thread-pool resources is by means of Rule FORK-R-★. In other words, thread-pool resources can only describe forked threads but not the *main thread* e_r on the specification side of the refinement. As we are going to see, the proof of *runForkSpec* needs access to the thread-pool resource describing the main thread. Rule REL-SPLIT from Vindum et al. [56, Fig. 8] supports this very feature. However, the statement relies on the fact that ReLoC's notion of refinement $\Delta \vDash e_l \precsim e_r : \tau$ is defined using $i \Rrightarrow e_r$ as a premise. This makes the adaption of REL-SPLIT to blaze particularly difficult, because blaze's model hides thread-pool assertions under multiple layers of abstraction.[5] Instead, we introduce Rule THREAD-SWAP-★ (Figure 2), which allows the user to trade a thread-pool resource $i \Rrightarrow K[e_r]$ in exchange for a thread-pool resource $j \Rrightarrow K'[e_r']$ describing the main thread e_r' under an abstract context K'. The expression e_r becomes the new main thread on the specification side and the postcondition is updated to require the termination of e_r', which is part of the implicit requirements of the original refinement.

3.1.2 Verification. After the allocation of an effect label $\$\mathtt{Fork}$ by *run_fork*, the crux of the proof is (1) the introduction of a relational theory *Fork* to relate $\$\mathtt{Fork}$ effects to **fork** and (2) the definition of the queue invariant in blaze. These definitions appear in Figure 3.

The theory *Fork* requires task_1 to refine task_2 as naturally expected. To allow $\$\mathtt{Fork}$ effects in task_1, the refinement between task_1 and task_2 assumes the theory *Fork* itself. The later modality $\triangleright$ guards this recursive occurrence of *Fork* to facilitate the definition in Iris. The return condition asserts that both the $\$\mathtt{Fork}$ effect and **fork** return `()`.

Recall that, according to the informal explanation of *run_fork*, the queue stores continuations that can be readily resumed. The definition of the queue invariant, the predicate *queueInv*, formalises this description. The term q represents the queue identifier. The term ks describes the contents of q. Concretely, it is a list of triples $(k,\ (j,\ K))$, where k is one of the continuations in q. This connection is captured by $\mathit{isQueue}(q,\ \mathit{ks}.1)$, which asserts q contains the collection of continuations

[5] The same holds for baze.

```
run_coop1 ≜ fun main.
  let effect Coop in
  let q = new_queue() in
  let next = fun _.
    if empty q then () else (pop q) () in
  let run = rec run p task. handle task() with
    | effect Coop request, k ⇒
        match request with
        | inl task' ⇒
          let p' = ref (inr []) in
          push q (fun _. k p'); run p' task'
        | inr p' ⇒ match !p' with
          | inl x ⇒ k x
          | inr ks ⇒ p' ← inr (k :: ks); next()
    | y ⇒
        let (inr ks) = !p in p ← inl y;
        iter (fun k. push q (fun _. k y)) ks;
        next()
  in
  let async = fun task'. perform Coop (inl task') in
  let await = fun p'. perform Coop (inr p') in
  let p = ref (inr []) in
  run p (fun _. main async await)
```

```
run_coop2 ≜ fun main.
  let effect Await in
  let new_promise = fun _.
    (ref (inr []), new_lock())
  in
  let run = rec run p task.
    handle task() with
    | effect Await p', k ⇒
        acquire p'.2; match !p'.1 with
        | inl x ⇒ release p'.2; k x
        | inr ks ⇒ p'.1 ← inr (k :: ks);
          release p'.2
    | y ⇒ acquire p.2;
        let (inr ks) = !p.1 in
        p.1 ← inl y; release p.2;
        iter (fun k. fork (k y)) ks
  in let async = fun task'.
    let p' = new_promise() in
    fork (run p' task'); p'
  in
  let await = fun p'. perform Await p' in
  let p = new_promise() in
  run p (fun _. main async await)
```

Fig. 4. Async/await implementations.

in ks. Because the continuation k is created by a running task that performs an effect, there must be a corresponding task on the specification side that k refines. The thread identifier j and the context K are used to describe the state of this task: it is an expression e_r such that $j \Mapsto K[e_r]$. Finally, the term ks' in *queueInv* represents the tasks on the specification side that have terminated and that were once used in the description of continuations in ks.

During the handling of a `$Fork` effect with payload $task_1'$, the specification side is a program of the form $K_r[\mathbf{fork}\ (task_2'())]$. After the application of Rule FORK-R-$\star$, the newly obtained resource $i \Mapsto task_2'()$ is immediately traded, via Rule THREAD-SWAP, for a thread-pool resource $j \Mapsto K'[K_r[()]]$ describing the main thread. This resource is used to show the queue invariant is preserved after pushing k. The proof then carries on with $run\ task_1'$ on the implementation side and the specification side correctly adjusted to $task_2'()$. Upon termination of a task, if the queue is non-empty, a continuation k is taken from the queue. At this point, Rule LOGICAL-FORK is used in conjunction with the thread-pool resource and the *ready* assumption retrieved from the queue invariant, thus concluding the proof.

3.1.3 Async/await. We prove a similar refinement statement for an *asynchronous-computation* library offering *async* and *await* effects [15, 18]. The implementation run_coop_1, which appears in Figure 4 is the translation to λ-blaze of the OCaml implementation from Dolan et al. [18, Fig. 1].

In addition to a queue of ready continuations, run_coop_1 also stores continuations in *promises*. Abstractly, a promise p represents the result of a running task. The continuations in p wait for this result. The continuations can be readily resumed once the task finishes, so they are transferred to

the queue. We show that run_coop_1 refines run_coop_2, which offers a more direct implementation of async using **fork** instead of storing continuations in a queue. The implementation of await by run_coop_2 still relies on a handler and also uses promises to manage waiting threads. To avoid races, run_coop_2 uses locks to protect accesses to promises.

The proof that run_coop_1 refines run_coop_2 relies on a queue invariant similar to *queueInv* (Figure 3). Other logical definitions used internally in the proof are adapted from de Vilhena and Pottier [15] (who carry out the verification of a similar asynchronous library in a unary setting in Iris). The complete list of definitions is included in the Appendix (§C.2.1).

Finally, we also prove the negative result that run_coop_1 *does not* refine the following handler-free implementation of async and await by run_coop_3, where async is implemented using **fork** and await is implemented by *busy waiting*:

```
deadlock ≜ fun async await.
  let r = ref (inl ()) in
  let p = async (rec f ().
    match !r with
    | inl () ⇒ async (fun _. ()); f()
    | inr p ⇒ await p
  ) in r ← inr p; await p
```

```
run_coop3 ≜ fun main.
  let async = fun task.
    let p = ref (inl ()) in
    fork (let y = task() in p ← (inr y)); p
  in let await = rec await p.
    match !p with inl () ⇒ await p | inr v ⇒ v
  in main async await
```

The key idea is to adapt the *deadlock* example from de Vilhena [14, Fig. 4.2] to exhibit a client that terminates when using the handler-based library but diverges otherwise.[6] In short, the client *deadlock* creates a cyclic dependency between p and itself. With the implementation of async and await by run_coop_3, when *deadlock* executes the final instruction *await p*, it diverges, because p is never fulfiled. With the implementation of async and await by run_coop_1, on the other hand, when *deadlock* executes the final instruction *await p*, it is captured in a continuation and stored in p. The internal queue managed by run_coop_1 becomes empty, so it terminates.

3.2 Algebraic effects: Haskell-like non-determinism

In this case study, we are interested in evaluating how relational theories can be used to reason about *algebraic effects* [42]. As an illustration, we consider the pair of constructs **or** and **fail**, where e_1 **or** e_2 models the functionality to non-deterministically run e_1 or e_2, and **fail** represents a failed execution path. These constructs are written in λ-blaze using a global effect `$ND`: e_1 **or** $e_2 \triangleq$ `(perform $ND (inl (fun _. e1, fun _. e2)))()` and **fail** $\triangleq$ `perform $ND (inr ())`.

The construct e_1 **or** e_2 performs a `$ND` effect with thunked versions of e_1 and e_2. After one of them is non-deterministically chosen by the handler, its execution is forced with `()`. The construct **fail** just performs a `$ND` effect.

Plotkin and Pretnar [44] show that **or** and **fail** can be described by the *algebraic theory* of a *monoid*: e_1 **or** (e_2 **or** e_3) = (e_1 **or** e_2) **or** e_3 and e **or** **fail** = **fail** **or** $e = e$. Such an algebraic theory can be used not only to reason about **or** and **fail** but also to state the correctness of an effect handler providing an implementation of these effects. In short, a handler is correct when the handling of two programs, that are equal according to the algebraic theory, yields equal results.

This equational correctness criterion suits a pure setting well, but precludes its application to cases where the effects **or** and **fail** are implemented using native non-determinism. For example, consider the two handler implementations that appear in Figure 5. The implementation of e_1 **or** e_2 provided by *run_nd_pure* uses a list to collect the results of returning e_1 and the results of returning e_2. Paths signalled by **fail** are not added to this list.[7] The implementation of e_1 **or** e_2 provided

[6] The precise statement is included in the Appendix (§C.2.2).

[7] This implementation is similar to the list instance of `MonadPlus`'s `mplus` and `mzero` [24].

```
run_nd_pure ≜ fun main.
  handle main() with
  | effect $ND request, k ⇒
      match request with
      | inl (t1, t2) ⇒ k t1 ++ k t2
      | inr () ⇒ []
  | y ⇒ [y]

run_nd_rand ≜ fun main. handle main() with
  | effect $ND request, k ⇒
      match request with
      | inl (t1, t2) ⇒ let b = ref true in
          fork (b ← false); if !b then k t1 else k t2
      | inr () ⇒ (rec f (). f())()
  | y ⇒ y
```

Fig. 5. Non-determinism handlers.

by *run_nd_rand* chooses the expression to run by reading a location b that holds `true` initially but is non-deterministically set to `false` by a forked thread.[8] The handling of **fail** diverges.

The correctness criterion of Plotkin and Pretnar [44] can be used to justify *run_nd_pure* provides a correct implementation of **or** and **fail** with respect to their algebraic theory. However, *run_nd_rand* falls out of the scope of their approach. Using relational theories of blaze, it is possible to introduce a similar handler-correctness criterion applicable to both *run_nd_pure* and *run_nd_rand*:

$$\mathit{runNdCorrect}(\mathit{run}) \triangleq \begin{array}{l}\forall \mathit{main}_1, \\ \mathit{main}_2,\ \mathcal{L}.\end{array} \begin{cases} \mathit{main}_1\,() \lesssim_\star \mathit{main}_2\,() \ \langle([\$\mathsf{ND}],\ [\$\mathsf{ND}],\ \mathit{Nd}) :: \mathcal{L}\rangle\ \{=\} \twoheadrightarrow \\ \mathit{run}\ \mathit{main}_1 \lesssim_\star \mathit{run}\ \mathit{main}_2\ \langle([\$\mathsf{ND}],\ [\$\mathsf{ND}],\ \bot) :: \mathcal{L}\rangle\ \{=\} \end{cases}$$

The predicate $\mathit{runNdCorrect}(\mathit{run})$ asserts the correctness of a handler *run* with respect to a relational theory *Nd*. It states that the handling of two handlees main_1 and main_2 yields the same results assuming main_1 and main_2 are related under the theory *Nd* for `$ND`. The handler *run* cannot itself rely on `$ND` and it must not intercept other effects related by $\mathcal{L}$. The theory *Nd* enables algebraic reasoning about **or** and **fail**. It is written as the sum of several theories expressing their algebraic laws: $\mathit{Nd} \triangleq \mathit{Assoc}_1 \oplus \mathit{Assoc}_2 \oplus \mathit{Unit}_1 \oplus \mathit{Unit}_2 \oplus \mathit{Unit}_3 \oplus \mathit{Unit}_4 \oplus \mathit{Refl}_1 \oplus \mathit{Refl}_2$, where

$$\mathit{Assoc}_1(e_{11}\ \mathbf{or}\ (e_{12}\ \mathbf{or}\ e_{13}),\ (e_{21}\ \mathbf{or}\ e_{22})\ \mathbf{or}\ e_{23},\ Q) \triangleq \Box Q(e_{11}, e_{21}) * \Box Q(e_{12}, e_{22}) * \Box Q(e_{13}, e_{23})$$

$$\mathit{Assoc}_2((e_{11}\ \mathbf{or}\ e_{12})\ \mathbf{or}\ e_{23},\ e_{21}\ \mathbf{or}\ (e_{22}\ \mathbf{or}\ e_{23}),\ Q) \triangleq \Box Q(e_{11}, e_{21}) * \Box Q(e_{12}, e_{22}) * \Box Q(e_{13}, e_{23})$$

$$\mathit{Unit}_1(e_1\ \mathbf{or}\ \mathbf{fail},\ e_2,\ Q) \triangleq \mathit{Unit}_2(\mathbf{fail}\ \mathbf{or}\ e_1,\ e_2,\ Q) \triangleq \Box Q(e_1, e_2)$$

$$\mathit{Unit}_3(e_1,\ e_2\ \mathbf{or}\ \mathbf{fail},\ Q) \triangleq \mathit{Unit}_4(e_1,\ \mathbf{fail}\ \mathbf{or}\ e_2,\ Q) \triangleq £1 * \Box Q(e_1, e_2)$$

$$\mathit{Refl}_1(e_{11}\ \mathbf{or}\ e_{12},\ e_{21}\ \mathbf{or}\ e_{22},\ Q) \triangleq \Box Q(e_{11}, e_{21}) * \Box Q(e_{12}, e_{22})$$

$$\mathit{Refl}_2(\mathbf{fail},\ \mathbf{fail},\ \_) \triangleq \mathsf{True}$$

The theory Assoc_1 captures the associativity of **or**. The return condition Q is used to express the condition that the relation holds up to a relation of the subexpressions. The other theories are written in a similar style, except for Unit_3 and Unit_4, which charge the user one *later credit* [48], part of Iris's machinery to avoid cyclic proofs. Without the charge of one later credit, the theory Unit_4, for example, could be used to relate a terminating e_1 to a diverging e_2 such as `(rec f (). fail or f())()`. This claim is formally proved [17].

As noted in §1, blaze cannot express algebraic theories that are closed under transitivity. Therefore, *Nd* is symmetric and reflexive, but not transitive. The lack of support for transitivity is a known limitation of step-indexed relational logics [8, 26]. *Nd* is however sufficiently expressive to relate non-trivial examples of handlees (§C.3). Using the *runNdCorrect* correctness criterion, we show that both *run_nd_pure* and *run_nd_rand* are correct with respect to *Nd*: $\mathit{runNdCorrect}(\mathit{run\_nd\_pure})$ and $\mathit{runNdCorrect}(\mathit{run\_nd\_rand})$ hold.

[8] This implementation is originally given by Frumin et al. [22, §6.4].

4 Related Work

To our knowledge, this is the first work to introduce a relational separation logic for effect handlers. In the following paragraphs, we discuss work within closely related topics.

Relational reasoning about effect handlers. Building on the notion of *algebraic effects*, where an effect is described by an equational theory, Plotkin and Pretnar [44] introduce the notion of correctness of handlers whereby the handler of an effect is correct if the handler *respects* the equations describing this effect. This equational approach is well-suited to strictly functional programs but has never been extended to languages with concurrency and mutable state. We follow a different approach, namely relational separation logic, but take inspiration from equational reasoning to introduce a notion of handler correctness that supports these features (§3.2).

Biernacki et al. [5] introduce binary logical relations for effect handlers. Their *biorthogonal-closed* [41] style of relations inspires similar definitions by several authors [7, 39, 57]. Such binary logical relations can be used as an intermediary step in the proof of contextual refinement. Biernacki et al. [5] explore this approach to establish interesting examples of refinement, including a statement about the *ask effect* [5, §4.1], similar to the one studied in **??**, and one about the *state effect* [5, §4.2], ported to our system in our Rocq formalisation.

Logical relations can be used to develop high-level reasoning principles. Biernacki et al. [5]'s Lemma 2, for example, can be seen as a form of bind rule. The main limitation of previous logical-relations approaches is the lack of a comprehensive set of such high-level reasoning rules with which the user can verify relational properties of programs with handlers without ever being exposed to details of the model of the logic. Using separation logic as the foundation of our logic also has the advantage of having a richer assertion language than a language limited to the interpretation of syntactic types. Such expressivity is key in adding support for higher-order store and concurrency. (Even though the latter, as discussed in §3.1.1, required original work.)

Relational reasoning about continuations in Iris. Timany and Birkedal [53] devise binary logical relations for programs that manipulate *undelimited continuations* captured by `callcc`. They use these logical relations to verify multiple challenging examples of refinement, one of which is similar to the fork library we verify in §3.1. Namely, they show that the `callcc`-based implementation of fork written in a sequential language refines the **`fork`** construct of a language with native cooperative concurrency. The refinement therefore relates programs written in different languages. To carry out this refinement, they devise *cross-language* logical relations. Like previous works exploiting logical relations, and unlike our work, the lack of a comprehensive set of high-level reasoning rules necessitates the proofs to be carried out at the level of Iris's weakest precondition *wp*, which, in their setting, is inconvenient because, in the presence of `callcc`, the bind rule for their version of *wp* is unsound. They mitigate this inconvenience by introducing the *context-local weakest precondition*, which admits the bind rule for the price of reduced support for `callcc`. (Although notions of weakest precondition that admit the bind rule while keeping convenient support for `callcc` exist [14, §6.3.2].)

Relational theories. de Vilhena and Pottier [15] introduce *protocols* as a mechanism to allow modular reasoning about programs with effect handlers in a unary setting. The domain of relational theories *iThy* (**??**) can be seen as a generalisation to a binary setting of the domain of protocols [15, Fig. 4] $(Val \to (Val \to iProp)) \to iProp$. An immediate generalisation is to replace *Val* with a binary type $Val \times Val$. A more subtle generalisation is to subsequently replace *Val* with *Expr*. This is needed to allow relations between effectful and non-effectful expressions. For the same reason, Biernacki et al. [5] introduce a similar domain of *semantic effects* **Eff** [5, §3.2], defined as a predicate of type $(Expr^2 \times (Expr^2 \to SProp)) \to SProp$, where *SProp* is a type of *step-indexed assertions*. Allain

et al. [2] introduce a domain of protocols in Iris that coincides exactly with *iThy*. However, their focus is on the proof of correctness of compiler optimisations in a fragment of OCaml without handlers. Consequently, they derive a notion of simulation that admits a general bind rule with no conditions on contexts. To validate this rule, their simulation relation, by default, closes protocols under arbitrary evaluation contexts. In baze, we opt for a more flexible context-local reasoning principle where the user can choose when and under which contexts to close theories via the context-closure operator (**??**). This flexibility is key in the layered construction of blaze.

Reasoning about dynamic labels. de Vilhena and Pottier [16] introduce TesLogic, a unary logic for effect handlers with dynamic labels in a language similar to λ-blaze. The model of blaze is inspired by how TesLogic builds on top of Hazel [15], a unary logic for handlers which, like baze, lacks the abstraction principles for dynamic labels. The rules of TesLogic [14, Fig. 7.2], however, differ from the ones in blaze in key ways: whereas they have an explicit rule to reason about handlers, Rule EXHAUSTION-$\star$ can be applied to contexts without handlers; and, whereas their bind rule is limited to neutral contexts, Rule BIND-$\star$ can be applied to contexts with handlers.

Flexible relational reasoning rules for concurrency. Like Vindum et al. [56], we notice limitations of the reasoning rules for concurrency provided by standard relational separation logic. We have already compared the differences between our approaches in §3.1.1. In short, we both rely on *ghost thread-pool* assertions $i \Longmapsto e$ describing the state of thread i on the specification side. However, while their rules require the user to explicitly execute e, our rules use the assertions $i \Longmapsto e$ merely as tokens that can be forged, spent, or exchanged during the construction of a proof.

5 Future Work

Limitations of our current framework indicate directions for future work. An important deficiency is the lack of a type system. In a relational setting, a type system is particularly useful, because it offers a syntax-directed approach to prove refinements of the form $e \precsim e$. In the future, we would like to remedy this deficiency by extending λ-blaze with a type system for handlers with dynamic labels, such as Tes [16]. It would be interesting to see how blaze could be used to devise a binary-logical-relations interpretation of Tes and whether the resulting interpretation could be used to show Tes enforces abstraction principles for programming with handlers, such as the *absence of accidental handling* [57, 58]. Finally, we would like to explore alternative definitions of the model. We suspect the later modality in the definition of baze's refinement relation can be eliminated by using an alternative method for constructing recursive definitions, namely Iris's *greatest fixpoint operator* [35, 51]. Following recent work [2, 23], we would also like to investigate the implications of generalising the type of postconditions to a predicate on pairs of expressions. We believe this generalisation could improve context-local reasoning by allowing our bind rules (BIND and BIND-$\star$) to focus on pairs of expressions that do not necessarily terminate synchronously.

References

[1] Amal J. Ahmed, Andrew W. Appel, and Roberto Virga. 2002. A Stratified Semantics of General References Embeddable in Higher-Order Logic. In *Logic in Computer Science (LICS)*. 75–86. doi:10.1109/LICS.2002.1029818

[2] Clément Allain, Frédéric Bour, Basile Clément, François Pottier, and Gabriel Scherer. 2025. Tail Modulo Cons, OCaml, and Relational Separation Logic. In *Principles of Programming Languages (POPL)*, Vol. 9. ACM Press. doi:10.1145/3704915

[3] Andrew W. Appel, Paul-André Melliès, Christopher D. Richards, and Jérôme Vouillon. 2007. A very modal model of a modern, major, general type system. In *Principles of Programming Languages (POPL)*. 109–122. doi:10.1145/1190216.1190235

[4] Andrej Bauer and Matija Pretnar. 2014. An Effect System for Algebraic Effects and Handlers. *Logical Methods in Computer Science* 10, 4 (2014). doi:10.2168/LMCS-10(4:9)2014

[5] Dariusz Biernacki, Maciej Piróg, Piotr Polesiuk, and Filip Sieczkowski. 2018. Handle with care: relational interpretation of algebraic effects and handlers. *Proceedings of the ACM on Programming Languages* 2, POPL (2018), 8:1–8:30. doi:10.1145/3158096

[6] Dariusz Biernacki, Maciej Piróg, Piotr Polesiuk, and Filip Sieczkowski. 2019. Abstracting algebraic effects. *Proceedings of the ACM on Programming Languages* 3, POPL (2019), 6:1–6:28. doi:10.1145/3290319

[7] Dariusz Biernacki, Maciej Piróg, Piotr Polesiuk, and Filip Sieczkowski. 2020. Binders by day, labels by night: effect instances via lexically scoped handlers. *Proceedings of the ACM on Programming Languages* 4, POPL (2020), 48:1–48:29. doi:10.1145/3371116

[8] Lars Birkedal and Aleš Bizjak. 2012. A note on the transitivity of step-indexed logical relations. (Nov. 2012). https://abizjak.github.io/documents/notes/step-indexed-transitivity.pdf

[9] John Boyland. 2003. Checking Interference with Fractional Permissions. In *Static Analysis Symposium (SAS) (Lecture Notes in Computer Science, Vol. 2694)*. 55–72. doi:10.1007/3-540-44898-5_4

[10] Jonathan Immanuel Brachthäuser, Philipp Schuster, and Klaus Ostermann. 2020. Effekt: Capability-passing style for type- and effect-safe, extensible effect handlers in Scala. *Journal of Functional Programming* 30 (2020), e8. doi:10.1017/S0956796820000027

[11] Edwin C. Brady. 2013. Programming and reasoning with algebraic effects and dependent types. In *International Conference on Functional Programming (ICFP)*. 133–144. doi:10.1145/2500365.2500581

[12] Ezra Cooper, Sam Lindley, Philip Wadler, and Jeremy Yallop. 2006. Links: Web Programming Without Tiers. In *Formal Methods for Components and Objects (Lecture Notes in Computer Science, Vol. 4709)*. 266–296. doi:10.1007/978-3-540-74792-5_12

[13] Ana Lúcia de Moura and Roberto Ierusalimschy. 2009. Revisiting Coroutines. *ACM Transactions on Programming Languages and Systems* 31, 2 (Feb. 2009), 1–31. doi:10.1145/1462166.1462167

[14] Paulo Emílio de Vilhena. 2022. *Proof of Programs with Effect Handlers*. Ph. D. Dissertation. Université Paris Cité. https://inria.hal.science/tel-03891381

[15] Paulo Emílio de Vilhena and François Pottier. 2021. A Separation Logic for Effect Handlers. *Proceedings of the ACM on Programming Languages* 5, POPL (Jan. 2021). doi:10.1145/3434314

[16] Paulo Emílio de Vilhena and François Pottier. 2023. A Type System for Effect Handlers and Dynamic Labels. In *European Symposium on Programming (ESOP) (Lecture Notes in Computer Science, Vol. 13990)*. 225–252. doi:10.1007/978-3-031-30044-8_9

[17] Paulo Emílio de Vilhena, Simcha van Collem, Ines Wright, and Robbert Krebbers. 2026. blaze - A Relational Separation Logic for Effect Handlers. https://github.com/DeVilhena-Paulo/blaze.

[18] Stephen Dolan, Spiros Eliopoulos, Daniel Hillerström, Anil Madhavapeddy, K. C. Sivaramakrishnan, and Leo White. 2017. Concurrent System Programming with Effect Handlers. In *Trends in Functional Programming (TFP) (Lecture Notes in Computer Science, Vol. 10788)*. 98–117. doi:10.1007/978-3-319-89719-6_6

[19] Derek Dreyer, Amal Ahmed, and Lars Birkedal. 2011. Logical Step-Indexed Logical Relations. *Logical Methods in Computer Science* 7, 2 (2011). doi:10.2168/LMCS-7(2:16)2011

[20] Ivana Filipovic, Peter W. O'Hearn, Noam Rinetzky, and Hongseok Yang. 2010. Abstraction for concurrent objects. *Theoretical Computer Science* 411, 51-52 (2010), 4379–4398. doi:10.1016/J.TCS.2010.09.021

[21] Dan Frumin, Robbert Krebbers, and Lars Birkedal. 2018. ReLoC: A Mechanised Relational Logic for Fine-Grained Concurrency. In *Logic in Computer Science (LICS)*. 442–451. doi:10.1145/3209108.3209174

[22] Dan Frumin, Robbert Krebbers, and Lars Birkedal. 2021. ReLoC Reloaded: A Mechanized Relational Logic for Fine-Grained Concurrency and Logical Atomicity. *Logical Methods in Computer Science* 17, 3 (2021). doi:10.46298/LMCS-17(3:9)2021

[23] Lennard Gäher, Michael Sammler, Simon Spies, Ralf Jung, Hoang-Hai Dang, Robbert Krebbers, Jeehoon Kang, and Derek Dreyer. 2022. Simuliris: a separation logic framework for verifying concurrent program optimizations. *Proceedings of the ACM on Programming Languages* 6, POPL (2022), 1–31. doi:10.1145/3498689

[24] Haskell Community. 2023. Alternative and MonadPlus. https://en.wikibooks.org/wiki/Haskell/Alternative_and_MonadPlus

[25] Daniel Hillerström and Sam Lindley. 2016. Liberating effects with rows and handlers. In *International Workshop on Type-Driven Development (TyDe@ICFP)*. 15–27. doi:10.1145/2976022.2976033

[26] Chung-Kil Hur, Derek Dreyer Georg, Neis, and Viktor Vafeiadis. 2012. The marriage of bisimulations and Kripke logical relations. In *Principles of Programming Languages (POPL)*. ACM Press, 59–72. doi:10.1145/2103656.2103666

[27] Ralf Jung, Robbert Krebbers, Lars Birkedal, and Derek Dreyer. 2016. Higher-order ghost state. In *International Conference on Functional Programming (ICFP)*. 256–269. doi:10.1145/2951913.2951943

[28] Ralf Jung, Robbert Krebbers, Jacques-Henri Jourdan, Aleš Bizjak, Lars Birkedal, and Derek Dreyer. 2018. Iris from the ground up: A modular foundation for higher-order concurrent separation logic. *Journal of Functional Programming* 28 (2018), e20. doi:10.1017/S0956796818000151

[29] Ralf Jung, David Swasey, Filip Sieczkowski, Kasper Svendsen, Aaron Turon, Lars Birkedal, and Derek Dreyer. 2015. Iris: monoids and invariants as an orthogonal basis for concurrent reasoning. In *Principles of Programming Languages (POPL)*. 637–650. doi:10.1145/2676726.2676980

[30] Ohad Kammar, Paul B. Levy, Sean K. Moss, and Sam Staton. 2017. A monad for full ground reference cells. In *Logic in Computer Science (LICS)*. doi:10.1109/LICS.2017.8005109

[31] Oleg Kiselyov and Hiromi Ishii. 2015. Freer monads, more extensible effects. In *Proceedings of the 2015 ACM SIGPLAN Symposium on Haskell (Haskell '15)*. 94–105. doi:10.1145/2804302.2804319

[32] Robbert Krebbers, Jacques-Henri Jourdan, Ralf Jung, Joseph Tassarotti, Jan-Oliver Kaiser, Amin Timany, Arthur Charguéraud, and Derek Dreyer. 2018. MoSeL: a general, extensible modal framework for interactive proofs in separation logic. *Proceedings of the ACM on Programming Languages* 2, ICFP (2018), 77:1–77:30. doi:10.1145/3236772

[33] Robbert Krebbers, Ralf Jung, Aleš Bizjak, Jacques-Henri Jourdan, Derek Dreyer, and Lars Birkedal. 2017. The essence of higher-order concurrent separation logic. In *European Symposium on Programming (ESOP) (Lecture Notes in Computer Science, Vol. 10201)*. 696–723. doi:10.1007/978-3-662-54434-1_26

[34] Robert Krebbers, Amin Timany, and Lars Birkedal. 2017. Interactive proofs in higher-order concurrent separation logic. In *Principles of Programming Languages (POPL)*. doi:10.1145/3009837.3009855

[35] Robbert Krebbers, Luko van der Maas, and Enrico Tassi. 2025. Inductive Predicates via Least Fixpoints in Higher-Order Separation Logic. In *Interactive Theorem Proving (ITP)*. doi:10.4230/LIPICS.ITP.2025.27

[36] Daan Leijen. 2014. Koka: Programming with Row Polymorphic Effect Types. In *Workshop on Mathematically Structured Functional Programming (MSFP)*, Vol. 153. 100–126. doi:10.4204/EPTCS.153.8

[37] Xavier Leroy, Damien Doligez, Alain Frisch, Jacques Garrigue, Didier Rémy, KC Sivaramakrishnan, and Jérôme Vouillon. 2025. The OCaml system: Documentation and user's manual. https://ocaml.org/manual/5.3/index.html

[38] Sam Lindley, Conor McBride, and Craig McLaughlin. 2017. Do Be Do Be Do. In *Principles of Programming Languages (POPL)*. doi:10.1145/3009837.3009897

[39] Craig McLaughlin. 2020. *Relational reasoning for effects and handlers.* Ph. D. Dissertation. University of Edinburgh, UK. doi:10.7488/ERA/537

[40] Peter W. O'Hearn, John C. Reynolds, and Hongseok Yang. 2001. Local Reasoning about Programs that Alter Data Structures. In *Computer Science Logic (Lecture Notes in Computer Science, Vol. 2142)*. 1–19. doi:10.1007/3-540-44802-0_1

[41] Andrew Pitts and Ian Stark. 1999. *Operational reasoning for functions with local state.* Cambridge University Press, 227—-274.

[42] Gordon D. Plotkin and Matija Pretnar. 2008. A Logic for Algebraic Effects. In *Logic in Computer Science (LICS)*. 118–129. https://homepages.inf.ed.ac.uk/gdp/publications/Logic_Algebraic_Effects.pdf

[43] Gordon D. Plotkin and Matija Pretnar. 2009. Handlers of Algebraic Effects. In *European Symposium on Programming (ESOP) (Lecture Notes in Computer Science, Vol. 5502)*. 80–94. doi:10.1007/978-3-642-00590-9_7

[44] Gordon D. Plotkin and Matija Pretnar. 2013. Handling Algebraic Effects. *Logical Methods in Computer Science* 9, 4 (Dec. 2013). https://lmcs.episciences.org/705

[45] Matija Pretnar. 2015. An Introduction to Algebraic Effects and Handlers. In *Mathematical Foundations of Programming Semantics (Electronic Notes in Theoretical Computer Science, Vol. 319)*. Elsevier, 19–35. doi:10.1016/J.ENTCS.2015.12.003

[46] John C. Reynolds. 2002. Separation Logic: A Logic for Shared Mutable Data Structures. In *Logic in Computer Science (LICS)*. 55–74. doi:10.1109/LICS.2002.1029817

[47] Alex Simpson and Niels Voorneveld. 2019. Behavioural Equivalence via Modalities for Algebraic Effects. *ACM Transactions on Programming Languages and Systems* 42 (Nov. 2019). doi:10.1145/3363518

[48] Simon Spies, Lennard Gäher, Joseph Tassarotti, Ralf Jung, Robbert Krebbers, Lars Birkedal, and Derek Dreyer. 2022. Later credits: resourceful reasoning for the later modality. In *International Conference on Functional Programming (ICFP)*. doi:10.1145/3547631

[49] Wenhao Tang, Daniel Hillerström, Sam Lindley, and Garrett J. Morris. 2024. Soundly Handling Linearity. In *Principles of Programming Languages (POPL)*, Vol. 8. ACM Press, 1600—-1628. doi:10.1145/3632896

[50] Wenhao Tang, Leo White, Stephen Dolan, Daniel Hillerström, Sam Lindley, and Anton Lorenzen. 2025. Modal Effect Types, In Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA). *Proceedings of the ACM on Programming Languages* 9. doi:10.1145/3720476

[51] The Iris Team. 2025. Iris Fixpoint Operators. https://gitlab.mpi-sws.org/iris/iris/-/blob/master/iris/bi/lib/fixpoint_mono.v

[52] The Rocq Prover development team. 2025. *The Rocq Prover.* https://rocq-prover.org/

[53] Amin Timany and Lars Birkedal. 2019. Mechanized Relational Verification of Concurrent Programs with Continuations. *Proceedings of the ACM on Programming Languages* 3, ICFP (July 2019), 105:1–105:28. doi:10.1145/3341709

[54] Orpheas van Rooij and Robbert Krebbers. 2025. Affect: An Affine Type and Effect System. In *Principles of Programming Languages (POPL)*, Vol. 9. ACM Press, Article 5, 29 pages. doi:10.1145/3704841

[55] Simon Friis Vindum and Lars Birkedal. 2021. Contextual refinement of the Michael-Scott queue. In *Certified Programs and Proofs (CPP)*. 76–90. doi:10.1145/3437992.3439930

[56] Simon Friis Vindum, Dan Frumin, and Lars Birkedal. 2022. Mechanized verification of a fine-grained concurrent queue from Meta's Folly library. In *Certified Programs and Proofs (CPP)*. ACM Press, 100—-115. doi:10.1145/3497775.3503689

[57] Yizhou Zhang and Andrew C. Myers. 2019. Abstraction-safe effect handlers via tunneling. In *Principles of Programming Languages (POPL)*, Vol. 3. ACM Press, 5:1–5:29. doi:10.1145/3290318

[58] Yizhou Zhang, Guido Salvaneschi, Quinn Beightol, Barbara Liskov, and Andrew C. Myers. 2016. Accepting blame for safe tunneled exceptions. In *Programming Language Design and Implementation (PLDI)*. 281–295. doi:10.1145/2908080.2908086

A Language

$$
\begin{array}{rcl}
e & ::= & v \mid x \mid e\,e \mid \mathbf{let}\ x = e\ \mathbf{in}\ e \mid (e, e) \\
& \mid & e.1 \mid e.2 \mid \mathbf{if}\ e\ \mathbf{then}\ e\ \mathbf{else}\ e \\
& \mid & \begin{array}{l}\mathbf{match}\ e\ \mathbf{with} \\ \mid \mathbf{inl}\ x \Rightarrow e \mid \mathbf{inl}\ e \mid \mathbf{inr}\ e \\ \mid \mathbf{inr}\ y \Rightarrow e\end{array} \\
& \mid & \mathbf{let\,effect}\ \mathtt{E}\ \mathbf{in}\ e \mid \mathbf{perform}\ \mathtt{E}\ e \\
& \mid & \begin{array}{l}\mathbf{handle}\ e\ \mathbf{with} \\ \mid \mathbf{effect}\ \mathtt{E}\ x, \mathbf{rec}^?\ k\ \mathbf{as\,multi}^?\ \Rightarrow e \\ \mid y \Rightarrow e\end{array} \\
& \mid & \mathbf{ref}\ e \mid\ !e \mid e \leftarrow e \mid \mathbf{fork}\ e \mid \mathbf{cas}\ (e,e,e) \\
& \mid & \begin{array}{l}\mathbf{handle}\ e\ \mathbf{with} \\ \mid \mathbf{effect}\ \$\mathtt{E}\ x, \mathbf{rec}^?\ k\ \mathbf{as\,multi}^?\ \Rightarrow e \\ \mid y \Rightarrow e\end{array} \\
& \mid & \mathbf{perform}\ \$\mathtt{E}\ e
\end{array}
\qquad
\begin{array}{rcl}
v & ::= & () \mid \mathtt{true} \mid \mathtt{false} \mid n \mid \mathbf{rec}\ f\ x.\ e \mid (v, v) \\
& \mid & \mathbf{inl}\ v \mid \mathbf{inr}\ v \mid \ell \mid \mathbf{cont}\ \ell\ K \mid \mathbf{kont}\ K \\
K & ::= & [] \mid e\,K \mid K\,v \mid \mathbf{let}\ x = K\ \mathbf{in}\ e \\
& \mid & (e, K) \mid (K, v) \\
& \mid & K.1 \mid K.2 \mid \mathbf{if}\ K\ \mathbf{then}\ e\ \mathbf{else}\ e \\
& \mid & \begin{array}{l}\mathbf{match}\ K\ \mathbf{with} \\ \mid \mathbf{inl}\ x \Rightarrow e \mid \mathbf{inl}\ K \mid \mathbf{inr}\ K \\ \mid \mathbf{inr}\ y \Rightarrow e\end{array} \\
& \mid & \mathbf{perform}\ \$\mathtt{E}\ K \\
& \mid & \begin{array}{l}\mathbf{handle}\ K\ \mathbf{with} \\ \mid \mathbf{effect}\ \$\mathtt{E}\ x, \mathbf{rec}^?\ k\ \mathbf{as\,multi}^?\ \Rightarrow e \\ \mid y \Rightarrow e\end{array} \\
& \mid & \mathbf{ref}\ K \mid\ !K \mid e \leftarrow K \mid K \leftarrow v \\
& \mid & \mathbf{cas}\ (e,e,K) \mid \mathbf{cas}\ (e,K,v) \mid \mathbf{cas}\ (K,v,v)
\end{array}
$$

(a) Syntax of values, expressions, and evaluation contexts. (Runtime terms are displayed in gray.)

$$
\textsc{Effect}\ \frac{\{\vec{e}[i \mapsto K[\mathbf{let\,effect}\ \mathtt{E}\ \mathbf{in}\ e]];\sigma;\delta\} \quad \$\mathtt{E} \notin \delta}{\{\vec{e}[i \mapsto K[e\{\$\mathtt{E}/\mathtt{E}\}]];\sigma;\delta \uplus \{\$\mathtt{E}\}\}}
\qquad
\textsc{Fork}\ \frac{\{\vec{e}[i \mapsto K[\mathbf{fork}\ e]];\sigma;\delta\} \quad n = |\vec{e}|}{\{\vec{e}[i \mapsto K[()], n \mapsto e];\sigma;\delta\}}
$$

$$
\textsc{Alloc}\ \frac{\{\vec{e}[i \mapsto K[\mathbf{ref}\ v]];\sigma;\delta\} \quad \ell \notin \sigma}{\{\vec{e}[i \mapsto K[\ell]];\sigma[\ell \mapsto v];\delta\}}
\qquad
\textsc{Pure}\ \frac{e_1 \to_{\mathsf{p}} e_2 \quad \{\vec{e}[i \mapsto K[e_1]];\sigma;\delta\}}{\{\vec{e}[i \mapsto K[e_2]];\sigma;\delta\}}
$$

$$
\textsc{Handle-os}\ \frac{\begin{array}{c}H = \mathbf{handle}\ []\ \mathbf{with\,effect}\ \$\mathtt{E}\ x, \mathbf{rec}^?\ k \Rightarrow h \mid y \Rightarrow r \\ \$\mathtt{E} \notin \mathscr{L}(K') \qquad \ell \notin \sigma \qquad \sigma' = \sigma[\ell \mapsto \mathtt{true}] \\ K'' = \mathit{if}\ \mathit{deep}(H)\ \mathit{then}\ H[K']\ \mathit{else}\ K' \qquad w = \mathbf{cont}\ \ell\ K''\end{array}}{\{\vec{e}[i \mapsto K[H[K'[\mathbf{perform}\ \$\mathtt{E}\ v]]]];\sigma;\delta\} \longrightarrow \{\vec{e}[i \mapsto K[h\{v/x, w/k\}]];\sigma';\delta\}}
$$

(b) Operational rules.

$$
\textsc{Beta}\ (\mathbf{rec}\ f\ x.\ e)\ v \to_{\mathsf{p}} e\{(\mathbf{rec}\ f\ x.\ e)/f, v/x\}
\qquad
\textsc{Multi-shot}\ (\mathbf{kont}\ K)\ v \to_{\mathsf{p}} K[v]
$$

$$
\textsc{Handle-ms}\ \frac{H = \mathbf{handle}\ []\ \mathbf{with\,effect}\ \$\mathtt{E}\ x, \mathbf{rec}^?\ k\ \mathbf{as\,multi} \Rightarrow h \mid y \Rightarrow r \quad \$\mathtt{E} \notin \mathscr{L}(K) \qquad K' = \mathit{if}\ \mathit{deep}(H)\ \mathit{then}\ H[K]\ \mathit{else}\ K}{H[K[\mathbf{perform}\ \$\mathtt{E}\ v]] \to_{\mathsf{p}} h\{v/x, \mathbf{kont}\ K'/k\}}
$$

(c) Pure-reduction rules.

Fig. 6. Syntax and semantics of λ-blaze.

B Logic

B.1 Iris instantiation and derived resources

Name	Type	Purpose
implStore	$Auth(Loc \xrightarrow{fin} (DFrac \times Ag\,Val))$	Modelling of the implementation-side points-to connective ($\_ \mapsto_{\mathrm{i}} \_$).
implLbls	$Auth(Lbl \xrightarrow{fin} (DFrac \times Ag\,Unit))$	Modelling of the implementation-side label predicate ($label_{\mathrm{i}}(\_, \_)$).
specPool	$Auth(\mathbb{N} \xrightarrow{fin} Ex\,Expr)$	Modelling of the ghost thread-pool assertion ($\_ \Rightarrow \_$).
specStore	$Auth(Lbl \xrightarrow{fin} (DFrac \times Ag\,Val))$	Modelling of the specification-side points-to connective ($\_ \mapsto_{\mathrm{s}} \_$).
specLbls	$Auth(Lbl \xrightarrow{fin} (DFrac \times Ag\,Unit))$	Modelling of the specification-side label predicate ($label_{\mathrm{s}}(\_, \_)$).

Fig. 7. Global ghost variables.

$$
\begin{aligned}
&\mathit{forkPost} \triangleq \lambda\_.\ \mathrm{True}\\
&\mathit{stateInterp}(\sigma, \delta) \triangleq \mathit{ownStore}_{\mathrm{i}}(\sigma) * \mathit{ownLbls}_{\mathrm{i}}(\delta)\\
&\qquad \text{where}\ \ \mathit{ownStore}_{\mathrm{i}}(\sigma) \triangleq \boxed{\bullet \bigcup_{(\ell,v)\in\sigma} \{\ell \mapsto (1, \mathrm{ag}(v))\}}^{\mathit{implStore}}\\
&\qquad\qquad \mathit{ownLbls}_{\mathrm{i}}(\delta) \triangleq \boxed{\bullet \bigcup_{\$\mathsf{E}\in\sigma} \{\$\mathsf{E} \mapsto (1, \mathrm{ag}())\}}^{\mathit{implLbls}}\\
&\mathit{latersPerStep}(n) \triangleq n
\end{aligned}
$$

Fig. 8. Definition of Iris-instantiation-related predicates (*forkPost*, *stateInterp*, and *latersPerStep*).

$$
\begin{aligned}
&\mathit{specCtx} \triangleq \exists \rho.\ \boxed{\exists \vec{e}, \sigma, \delta.\ \ \rho \rightarrow^{*} \{\vec{e}; \sigma; \delta\} * \mathit{ownPool}_{\mathrm{s}}(\vec{e}) * \mathit{ownStore}_{\mathrm{s}}(\sigma) * \mathit{ownLbls}_{\mathrm{s}}(\delta)}^{\mathit{specN}}\\
&\quad \text{where}\ \ \mathit{ownPool}_{\mathrm{s}}(\vec{e}) \triangleq \boxed{\bullet \bigcup_{(i,e)\in\vec{e}} \{i \mapsto \mathrm{ex}(e)\}}^{\mathit{specPool}}\\
&\qquad\quad \mathit{ownStore}_{\mathrm{s}}(\sigma) \triangleq \boxed{\bullet \bigcup_{(\ell,v)\in\sigma} \{\ell \mapsto (1, \mathrm{ag}(v))\}}^{\mathit{specStore}}\\
&\qquad\quad \mathit{ownLbls}_{\mathrm{s}}(\delta) \triangleq \boxed{\bullet \bigcup_{\$\mathsf{E}\in\delta} \{\$\mathsf{E} \mapsto (1, \mathrm{ag}())\}}^{\mathit{specLbls}}\\
&\mathit{specN} \triangleq \texttt{'spec'} (\in \mathit{String})
\end{aligned}
$$

Fig. 9. Definition of *specCtx*.

$$
\begin{aligned}
&\ell \overset{dq}{\mapsto}_{\mathrm{i}} v \triangleq \boxed{\circ \{\ell \mapsto (dq, \mathrm{ag}(v))\}}^{\mathit{implStore}}\\
&\mathit{label}_{\mathrm{i}}(\$\mathsf{E}, dq) \triangleq \boxed{\circ \{\$\mathsf{E} \mapsto (dq, \mathrm{ag}())\}}^{\mathit{implLbls}}
\end{aligned}
\qquad
\begin{aligned}
&i \Rightarrow e \triangleq \boxed{\circ \{i \mapsto \mathrm{ex}(e)\}}^{\mathit{specStore}}\\
&\ell \overset{dq}{\mapsto}_{\mathrm{s}} v \triangleq \boxed{\circ \{\ell \mapsto (dq, \mathrm{ag}(v))\}}^{\mathit{specStore}}\\
&\mathit{label}_{\mathrm{s}}(\$\mathsf{E}, dq) \triangleq \boxed{\circ \{\$\mathsf{E} \mapsto (dq, \mathrm{ag}())\}}^{\mathit{specLbls}}
\end{aligned}
$$

Fig. 10. Implementation-side and specification-side resources.

B.2 blaze

$$\textsc{monotonicity-gen-}\star\quad \frac{e_l \precsim_\star e_r \,\langle \mathcal{L}\rangle\, \{R\} \qquad \mathcal{L} \sqsubseteq_\star \mathcal{M} \qquad \Box_m \forall v_l,\, v_r.\ R(v_l,\, v_r) \mathrel{-\!\!*} S(v_l,\, v_r)}{e_l \precsim_\star e_r \,\langle \bigcirc_m \mathcal{M}\rangle\, \{S\}}$$

$$\textsc{exhaustion-gen-}\star\quad \frac{\begin{array}{c} \mathscr{L}(K_l) \subseteq ls_l \qquad \mathscr{L}(K_r) \subseteq ls_r \\ e_l \precsim_\star e_r \,\langle \mathcal{M}\rangle\, \{R\} \qquad \mathcal{M} = (ls_l,\, ls_r,\, \mathcal{T}) :: \mathcal{L} \qquad \mathcal{N} = (ls_l,\, ls_r,\, \mathcal{F}) :: (\bigcirc_m \mathcal{L}) \\ \wedge \begin{cases} \Box_m \forall v_l,\, v_r.\ R(v_l,\, v_r) \mathrel{-\!\!*} K_l[v_l] \precsim_\star K_r[v_r] \,\langle \mathcal{N}\rangle\, \{S\} \\ \Box_m \forall e_l',\, e_r'.\ ((ls_l,\, ls_r) \Downarrow \mathcal{T}) \blacktriangleleft e_l' \precsim_\star e_r' \,\langle \mathcal{M}\rangle\, \{R\} \mathrel{-\!\!*} K_l[e_l'] \precsim_\star K_r[e_r'] \,\langle \mathcal{N}\rangle\, \{S\} \end{cases} \end{array}}{K_l[e_l] \precsim_\star K_r[e_r] \,\langle \mathcal{N}\rangle\, \{S\}}$$

$$\begin{array}{rcl} \bigcirc_m [] & \triangleq & [] \\ \bigcirc_m (ls_l,\, ls_r,\, \mathcal{T}) :: \mathcal{L} & \triangleq & (ls_l,\, ls_r,\, \bigcirc_m \mathcal{T}) :: \bigcirc_m \mathcal{L} \end{array}$$

Fig. 11. Generalised reasoning rules in blaze.

B.3 Soundness

Definition B.1 (Safe).

$$safe(e,\, \phi) \ \triangleq\ \forall e',\, \vec{e_f},\, \sigma,\, \delta.\ \left(\begin{array}{l} \{[0 \mapsto e]\,;\, \emptyset\,;\, \emptyset\} \rightarrow^* \\ \quad \{[0 \mapsto e'] \uplus \vec{e_f}\,;\, \sigma\,;\, \delta\} \end{array}\right) \implies \vee \begin{cases} e' \in Val \wedge \phi(e') \\ \exists e''.\ \begin{array}{r} \{[0 \mapsto e'] \uplus \vec{e_f}\,;\, \sigma\,;\, \delta\} \rightarrow \\ \{[0 \mapsto e''] \uplus \_\,;\, \_\,;\, \_\} \end{array} \end{cases}$$

Definition B.2 (Terminates).

$$terminates(e,\, \phi) \ \triangleq\ \exists v.\ \phi(v) \wedge \{[0 \mapsto e]\,;\, \emptyset\,;\, \emptyset\} \rightarrow^* \{[0 \mapsto v] \uplus \_\,;\, \_\,;\, \_\}$$

Theorem B.3. *If* $\vdash e_l \precsim e_r \,\langle \bot\rangle\, \{\ulcorner \phi \urcorner\}$, *then* $safe(e_l,\, \lambda v_l.\ terminates(e_r,\, \lambda v_r.\ \phi(v_l,\, v_r)))$.

C Case studies

C.1 State

Examples adapted from Biernacki et al. [5, §4.2]:

```
run_ask_tell ≜ fun main.
  let effect Ask in
  let effect Tell in
  let ask = fun _. perform Ask () in
  let tell = fun y. perform Tell y in
  let run_ask ≜ fun y main'. handle main'() with effect Ask (), k ⇒ k y | z ⇒ z in
  let run_tell ≜ fun main'.
    handle main'() with effect Tell y, k ⇒ run_ask y (fun _. k ()) | z ⇒ z
  in run_tell (fun _. run_ask 0 (fun _. main ask tell))
```

```
run_cell ≜ fun main.
  let effect Cell in
  let get = fun _. perform Cell (inl ()) in
  let set = fun y. perform Cell (inr y) in
  let run = fun main.
    handle main() with
    | effect Cell request, k ⇒ fun x.
        match request with
        | inl () ⇒ k x x
        | inr y ⇒ k () y
    | y ⇒ fun _. y
  in run (fun _. main get set) 0
```

C.2 Concurrency

$$\textsc{fork-l}\quad \frac{i \Rrightarrow e_r \qquad e_l \precsim e_r\ \{\mathsf{True}\} \qquad K_l[()] \precsim e_r' \langle \mathcal{T} \rangle\ \{R\}}{K_l[\mathbf{fork}\ e_l] \precsim e_r' \langle \mathcal{T} \rangle\ \{R\}} \qquad \textsc{fork-r}\quad \frac{\forall i.\ i \Rrightarrow e_r \mathrel{-\!\!*} e_l \precsim K_l[()] \langle \mathcal{T} \rangle\ \{R\}}{e_l \precsim K_l[\mathbf{fork}\ e_r] \langle \mathcal{T} \rangle\ \{R\}}$$

$$\textsc{logical-fork}\quad \frac{i \Rrightarrow K_r[e_r] \qquad e_l \precsim e_r\ \{R\} \qquad \forall v_l, v_r.\ R(v_l, v_r) \mathrel{-\!\!*} i \Rrightarrow K_r[v_r] \mathrel{-\!\!*} K_l[v_l] \precsim e_r' \langle \mathcal{T} \rangle\ \{S\}}{K_l[e_l] \precsim e_r' \langle \mathcal{T} \rangle\ \{S\}}$$

$$\textsc{thread-swap}\quad \frac{i \Rrightarrow K[e_r] \qquad \forall j, K'.\ j \Rrightarrow K'[e_r'] \mathrel{-\!\!*} e_l \precsim e_r\ \{v_l\ \_.\ \exists v_r'.\ j \Rrightarrow K'[v_r'] \ast R(v_l, v_r')\}}{e_l \precsim e_r' \langle \mathcal{T} \rangle\ \{R\}}$$

Fig. 12. Reasoning rules for concurrency in baze.

$$\mathit{runCoopSpec} \triangleq \Box \forall \mathit{main}_1, \mathit{main}_2. \left(\begin{array}{l} \Box \forall \mathit{async}_1, \mathit{async}_2, \mathit{await}_1, \mathit{await}_2, \mathit{promise}, \mathcal{L}. \\ \mathit{asyncSpec}(\mathit{async}_1, \mathit{async}_2, \mathit{promise}, \mathcal{L}) \mathrel{-\!\!*} \\ \mathit{awaitSpec}(\mathit{await}_1, \mathit{await}_2, \mathit{promise}, \mathcal{L}) \mathrel{-\!\!*} \\ \mathit{main}_1\ \mathit{async}_1\ \mathit{await}_1 \precsim_\star \mathit{main}_2\ \mathit{async}_2\ \mathit{await}_2 \langle \mathcal{L} \rangle\ \{\mathsf{True}\} \end{array} \right) \mathrel{-\!\!*} \begin{array}{l} \mathit{run\_coop}_1\ \mathit{main}_1 \precsim_\star \\ \mathit{run\_coop}_2\ \mathit{main}_2\ \{\mathsf{True}\} \end{array}$$

$$\mathit{asyncSpec}(\mathit{async}_1, \mathit{async}_2, \mathit{promise}, \mathcal{L}) \triangleq \Box \forall \mathit{task}_1, \mathit{task}_2, S.\ \mathit{task}_1() \precsim_\star \mathit{task}_2() \langle \mathcal{L} \rangle\ \{v_l\, v_r.\ \Box S(v_l, v_r)\} \mathrel{-\!\!*} \mathit{async}_1\ \mathit{task}_1 \precsim_\star \mathit{async}_2\ \mathit{task}_2 \langle \mathcal{L} \rangle\ \{p_1\, p_2.\ \Box \mathit{promise}(p_1, p_2, S)\}$$

$$\mathit{awaitSpec}(\mathit{await}_1, \mathit{await}_2, \mathit{promise}, \mathcal{L}) \triangleq \Box \forall p_1, p_2, S.\ \mathit{promise}(p_1, p_2, S) \mathrel{-\!\!*} \mathit{await}_1\, p_1 \precsim_\star \mathit{await}_2\, p_2 \langle \mathcal{L} \rangle\ \{v_l\, v_r.\ \Box S(v_l, v_r)\}$$

Fig. 13. Async/await case study: Specification.

Relational theory.

$$\mathit{Coop} \triangleq \mathit{Async} \oplus \mathit{Await}$$

$$\mathit{Async}(\texttt{perform}\ \texttt{\$Coop}\ (\texttt{inl}\ \mathit{task}_1),\ \texttt{fork}\ (\mathit{task}_2()),\ Q) \triangleq \exists S.\ \triangleright \mathit{task}_1() \precsim_\star \mathit{task}_2()\ \langle[([\texttt{\$Coop}],\ [\texttt{\$Await}],\ \mathit{Coop})]\rangle\ \{v_l\ v_r.\ \square S(v_l, v_r)\} * \forall p_1, p_2.\ \mathit{promise}(p_1, p_2, S) \mathrel{-\!\!*} Q(p_1, p_2)$$

$$\mathit{Await}(\texttt{perform}\ \texttt{\$Coop}\ (\texttt{inr}\ p_1),\ \texttt{perform}\ \texttt{\$Await}\ p_2,\ Q) \triangleq \exists S.\ \mathit{promise}(p_1, p_2, S) * \forall v_l, v_r.\ \square S(v_l, v_r) \mathrel{-\!\!*} Q(v_l, v_r)$$

$$\mathit{promise}(p_1, p_2, S) \triangleq \exists \tau.\ \mathit{inMap}(p_1, p_2, \tau, S)$$

Ghost resources.

$$\mathit{token}(\tau) \triangleq \boxed{\mathsf{ex}(\bullet)}^{\tau} \qquad \mathit{inMap}(p_1, p_2, \tau, S) \triangleq \boxed{\circ\{(p_1, p_2, \tau) \mapsto S\}}^{\mathit{map}} \qquad \mathit{isMap}(M) \triangleq \boxed{\bullet M}^{\mathit{map}}$$

Invariants and predicates.

$$\mathit{queueInv}(q, ks, ks') \triangleq \mathit{isQueue}(q, ks.1) * \left(\ast_{(k,(j,K))\in ks}.\ \exists e_r.\ j \Rrightarrow K[e_r] * \mathit{ready}(q, k(), e_r)\right) * \left(\ast_{(\_,(j,K))\in ks'}.\ \exists v_r.\ j \Rrightarrow K[v_r]\right)$$

$$\mathit{promiseInv} \triangleq \exists M.\ \mathit{isMap}(M) * \ast_{\{(p_1,p_2,\tau)\mapsto S\}\in M}.\ \vee \begin{cases} \exists v_l, v_r. & \begin{pmatrix} p_1 \mapsto_{\mathtt{i}} \texttt{inl}\ v_l * \square S(v_l, v_r) \\ p_2 \mapsto_{\mathtt{s}} \texttt{inl}\ v_r * \mathit{token}(\tau) \end{pmatrix} \\ \exists ks. & \begin{pmatrix} p_1 \mapsto_{\mathtt{i}} \texttt{inr}\ ks.1 \\ p_2 \mapsto_{\mathtt{s}} \texttt{inr}\ ks.2 \\ \ast_{(k_1,k_2)\in ks}.\ \mathit{waiting}(q, S, k_1, k_2) \end{pmatrix} \end{cases}$$

$$\mathit{ready}(q, e_l, e_r) \triangleq \forall ks, ks'.\ \triangleright \mathit{promiseInv} q \mathrel{-\!\!*} \triangleright \mathit{queueInv}(q, ks, ks') \mathrel{-\!\!*} e_l \precsim_\star e_r\ \langle[([\texttt{\$Coop}],\ [\texttt{\$Await}],\ \bot)]\rangle\ \{\mathit{queueInv}(q, [], ks +\!\!+ ks')\}$$

$$\mathit{waiting}(q, S, k_1, k_2) \triangleq \forall v_l, v_r.\ \square S(v_l, v_r) \mathrel{-\!\!*} \mathit{ready}(q, (k_1\, v_l), (k_2\, v_r))$$

Fig. 14. Async/await case study: Internal logical definitions.

C.2.1 *Async/await – Part I.*

C.2.2 *Async/await – Part II.*

Theorem C.1.

$$\mathit{terminates}(\mathit{run\_coop}_1\ \mathit{deadlock},\ \lambda\_.\ \mathsf{True})$$

Definition C.2.

$$\mathit{diverges}(e) \triangleq \mathit{safe}(e,\ \lambda\_.\ \mathsf{False})$$

Theorem C.3.

$$\mathit{diverges}(\mathit{run\_coop}_3\ \mathit{deadlock})$$

Corollary C.4.

$$\neg(\vdash \mathit{run\_coop}_1\ \mathit{deadlock} \precsim_\star \mathit{run\_coop}_3\ \mathit{deadlock}\ \{\mathsf{True}\})$$

C.3 Non-determinism

Example of a derivable refinement using the relational theory *Nd*:

$$\texttt{(let } x \texttt{ = 0 or (1 or 2) in if (fail or true) then } x \texttt{ or } (x+1) \texttt{ else fail)} \lesssim_\star$$
$$\texttt{(let } x \texttt{ = (0 or 1) or 2 in } x \texttt{ or } (x+1)\texttt{)} \langle([\$\mathrm{ND}], [\$\mathrm{ND}], \mathit{Nd}) :: \mathcal{L}\rangle \{=\}$$

C.4 Invariants

We follow ReLoC [22]'s approach to add support for invariants: we add two general rules for allocating and closing invariants and one rule for opening invariant per atomic instruction. Effectively, this approach consists of three steps:

(1) **Masks.** First, we make surgical changes to the model of baze to parameterize the refinement relation on *masks* [28, §2]. These surgical changes are shown in Figure 15. The model of blaze can then be accordingly modified in a straightforward way (Figure 16).

(2) **Invariant rules.** Then, based on this updated model, we state and prove rules for allocating, closing, and opening invariants (Figure 17). As noted, the rules for allocating and closing invariants are general, whereas the rules for opening invariants are specific to atomic instructions. The rules for closing and opening invariants depend on the *opaque* assertion *closeInv*, which is internally defined as follows:

$$\mathit{closeInv}_{\mathcal{N}}(P) \triangleq \triangleright P \;{}_{(\top \setminus \mathcal{N}\uparrow)}\!\Rrightarrow\!\!\divideontimes_{\top}\; \mathsf{True}$$

(3) **Step rules.** Finally, we must add rules to allow partial execution on the specification side of the refinement under an arbitrary mask $\mathcal{E}$. Such rules are necessary because, under the hood, partial-execution-style reasoning on the specification side requires opening the invariant $\mathit{spec}\mathcal{N}$ in *specCtx* (see the definition of *specCtx* in Figure 9). Therefore, to allow the application of such rules after opening an invariant $\boxed{P}^{\mathcal{N}}$, we must show that $\mathit{spec}\mathcal{N} \neq \mathcal{N}$, because, otherwise, we could be opening the same invariant twice. The updated rules appear in Figures 19 and 20.

$$\begin{aligned}
O_{\mathcal{E}}(e_l, e_r, S) &\triangleq \forall i, K.\ \mathit{specCtx} \mathrel{-\!\!*} i \Rightarrow K[e_r] \;{}_{\mathcal{E}}\!\Rrightarrow\!\!\divideontimes_{\top}\; \mathit{wp}\ e_l\ \{v_l.\ \exists v_r.\ i \Rightarrow K[v_r] \ast S(v_l, v_r)\} \\
e_l \lesssim e_r\ \langle\mathcal{T}\rangle\ \{R\}_{\mathcal{E}} &\triangleq \forall K_l, K_r, S.\ \{R\}\ K_l \lesssim K_r\ \langle\mathcal{T}\rangle\ \{S\} \mathrel{-\!\!*} O_{\mathcal{E}}(K_l[e_l], K_r[e_r], S) \\
\{R\}\ K_l \lesssim K_r\ \langle\mathcal{T}\rangle\ \{S\} &\triangleq \wedge \begin{cases} \forall v_l, v_r.\ R(v_l, v_r) \mathrel{-\!\!*} O_{\top}(K_l[v_l], K_r[v_r], S) \\ \forall e_l, e_r.\ \mathcal{T} \blacktriangleleft e_l \lesssim e_r\ \{R\} \mathrel{-\!\!*} O_{\top}(K_l[e_l], K_r[e_r], S) \end{cases} \\
\mathcal{T} \blacktriangleleft e_l \lesssim e_r\ \{R\} &\triangleq \exists Q.\ \mathcal{T}(e_l, e_r, Q) \ast \square \triangleright \forall e_l', e_r'.\ Q(e_l', e_r') \mathrel{-\!\!*} e_l' \lesssim e_r'\ \langle\mathcal{T}\rangle\ \{R\}_{\top}
\end{aligned}$$

Fig. 15. Model of baze with masks.

$$e_l \lesssim_\star e_r\ \langle\mathcal{L}\rangle\ \{R\}_{\mathcal{E}} \triangleq \mathit{valid}(\mathcal{L}) \mathrel{-\!\!*} e_l \lesssim e_r\ \langle \mathit{interp}(\mathcal{L})\rangle\ \{R\}_{\mathcal{E}}$$

Fig. 16. Model of blaze with masks.

$$\textsc{alloc-inv}\quad \frac{\triangleright P \qquad \boxed{P}^{\mathcal{N}} \twoheadrightarrow e_l \precsim e_r \langle \mathcal{T} \rangle \{R\}_{\mathcal{E}}}{e_l \precsim e_r \langle \mathcal{T} \rangle \{R\}_{\mathcal{E}}} \qquad \textsc{close-inv}\quad \frac{\mathit{closeInv}_{\mathcal{N}}(P) \qquad \triangleright P \qquad e_l \precsim e_r \langle \mathcal{T} \rangle \{R\}_{\top}}{e_l \precsim e_r \langle \mathcal{T} \rangle \{R\}_{(\top \setminus \mathcal{N}^{\uparrow})}}$$

$$\textsc{load-open-inv}\quad \frac{\boxed{P}^{\mathcal{N}} \qquad \triangleright P \twoheadrightarrow \mathit{closeInv}_{\mathcal{N}}(P) \twoheadrightarrow \exists v.\, \triangleright \ell \overset{q}{\mapsto}_{\mathtt{i}} v \ast \triangleright \left(\ell \overset{q}{\mapsto}_{\mathtt{i}} v \twoheadrightarrow K_l[v] \precsim e_r \langle \mathcal{T} \rangle \{R\}_{(\top \setminus \mathcal{N}^{\uparrow})} \right)}{K_l[\,!\ell] \precsim e_r \langle \mathcal{T} \rangle \{R\}_{\top}}$$

$$\textsc{store-open-inv}\quad \frac{\boxed{P}^{\mathcal{N}} \qquad \triangleright P \twoheadrightarrow \mathit{closeInv}_{\mathcal{N}}(P) \twoheadrightarrow \triangleright \ell \mapsto_{\mathtt{i}} \_ \ast \triangleright \left(\ell \mapsto_{\mathtt{i}} v \twoheadrightarrow K_l[()] \precsim e_r \langle \mathcal{T} \rangle \{R\}_{(\top \setminus \mathcal{N}^{\uparrow})} \right)}{K_l[\ell \leftarrow v] \precsim e_r \langle \mathcal{T} \rangle \{R\}_{\top}}$$

Fig. 17. Reasoning rules for allocating, closing, and opening invariants in baze.

$$\textsc{alloc-inv-}\bigstar\quad \frac{\triangleright P \qquad \boxed{P}^{\mathcal{N}} \twoheadrightarrow e_l \precsim_{\star} e_r \langle \mathcal{L} \rangle \{R\}_{\mathcal{E}}}{e_l \precsim_{\star} e_r \langle \mathcal{L} \rangle \{R\}_{\mathcal{E}}} \qquad \textsc{close-inv-}\bigstar\quad \frac{\mathit{closeInv}_{\mathcal{N}}(P) \qquad \triangleright P \qquad e_l \precsim_{\star} e_r \langle \mathcal{L} \rangle \{R\}_{\top}}{e_l \precsim_{\star} e_r \langle \mathcal{L} \rangle \{R\}_{(\top \setminus \mathcal{N}^{\uparrow})}}$$

$$\textsc{load-open-inv-}\bigstar\quad \frac{\boxed{P}^{\mathcal{N}} \qquad \triangleright P \twoheadrightarrow \mathit{closeInv}_{\mathcal{N}}(P) \twoheadrightarrow \exists v.\, \triangleright \ell \overset{q}{\mapsto}_{\mathtt{i}} v \ast \triangleright \left(\ell \overset{q}{\mapsto}_{\mathtt{i}} v \twoheadrightarrow K_l[v] \precsim_{\star} e_r \langle \mathcal{L} \rangle \{R\}_{(\top \setminus \mathcal{N}^{\uparrow})} \right)}{K_l[\,!\ell] \precsim_{\star} e_r \langle \mathcal{L} \rangle \{R\}_{\top}}$$

$$\textsc{store-open-inv-}\bigstar\quad \frac{\boxed{P}^{\mathcal{N}} \qquad \triangleright P \twoheadrightarrow \mathit{closeInv}_{\mathcal{N}}(P) \twoheadrightarrow \triangleright \ell \mapsto_{\mathtt{i}} \_ \ast \triangleright \left(\ell \mapsto_{\mathtt{i}} v \twoheadrightarrow K_l[()] \precsim_{\star} e_r \langle \mathcal{L} \rangle \{R\}_{(\top \setminus \mathcal{N}^{\uparrow})} \right)}{K_l[\ell \leftarrow v] \precsim_{\star} e_r \langle \mathcal{L} \rangle \{R\}_{\top}}$$

Fig. 18. Reasoning rules for allocating, closing, and opening invariants in baze.

$$\textsc{step-r-mask}\quad \frac{\mathit{spec}\mathcal{N}^{\uparrow} \subseteq \mathcal{E} \qquad e_r \to_{\mathtt{p}} e_r' \qquad e_l \precsim K[e_r'] \langle \mathcal{T} \rangle \{R\}_{\mathcal{E}}}{e_l \precsim K[e_r] \langle \mathcal{T} \rangle \{R\}_{\mathcal{E}}}$$

$$\textsc{load-r-mask}\quad \frac{\mathit{spec}\mathcal{N}^{\uparrow} \subseteq \mathcal{E} \qquad \ell \overset{q}{\mapsto}_{\mathtt{s}} v \qquad \ell \overset{q}{\mapsto}_{\mathtt{s}} v \twoheadrightarrow e_l \precsim K[v] \langle \mathcal{T} \rangle \{R\}_{\mathcal{E}}}{e_l \precsim K[\,!\ell] \langle \mathcal{T} \rangle \{R\}_{\mathcal{E}}} \qquad \textsc{store-r-mask}\quad \frac{\mathit{spec}\mathcal{N}^{\uparrow} \subseteq \mathcal{E} \qquad \ell \mapsto_{\mathtt{s}} \_ \qquad \ell \mapsto_{\mathtt{s}} v \twoheadrightarrow e_l \precsim K[()] \langle \mathcal{T} \rangle \{R\}_{\mathcal{E}}}{e_l \precsim K[\ell \leftarrow v] \langle \mathcal{T} \rangle \{R\}_{\mathcal{E}}}$$

Fig. 19. Specification-side rules under arbitrary masks in baze.

$$\textsc{step-r-mask-}\bigstar\quad \frac{\mathit{spec}\mathcal{N}^{\uparrow} \subseteq \mathcal{E} \qquad e_r \to_{\mathsf{p}} e_r' \qquad e_l \lesssim_\star K[e_r'] \langle \mathcal{T} \rangle \{R\}_{\mathcal{E}}}{e_l \lesssim_\star K[e_r] \langle \mathcal{T} \rangle \{R\}_{\mathcal{E}}}$$

$$\textsc{load-r-mask-}\bigstar\quad \frac{\mathit{spec}\mathcal{N}^{\uparrow} \subseteq \mathcal{E} \qquad \ell \overset{q}{\mapsto}_{\mathsf{s}} v \qquad \ell \overset{q}{\mapsto}_{\mathsf{s}} v \mathrel{-\!\!*} e_l \lesssim_\star K[v] \langle \mathcal{T} \rangle \{R\}_{\mathcal{E}}}{e_l \lesssim_\star K[!\ell] \langle \mathcal{T} \rangle \{R\}_{\mathcal{E}}}$$

$$\textsc{store-r-mask-}\bigstar\quad \frac{\mathit{spec}\mathcal{N}^{\uparrow} \subseteq \mathcal{E} \qquad \ell \mapsto_{\mathsf{s}} \_ \qquad \ell \mapsto_{\mathsf{s}} v \mathrel{-\!\!*} e_l \lesssim_\star K[()] \langle \mathcal{T} \rangle \{R\}_{\mathcal{E}}}{e_l \lesssim_\star K[\ell \leftarrow v] \langle \mathcal{T} \rangle \{R\}_{\mathcal{E}}}$$

Fig. 20. Specification-side rules under arbitrary masks in blaze.