LATTICE-BASED DATA STRUCTURES FOR DETERMINISTIC PARALLEL AND DISTRIBUTED PROGRAMMING

Lindsey Kuper

Submitted to the faculty of the University Graduate School
in partial fulfillment of the requirements
for the degree
Doctor of Philosophy
in the School of Informatics and Computing
Indiana University
August 2014

Accepted by the Graduate Faculty, Indiana University, in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

Ryan R. Newton, Ph.D.

Amr Sabry, Ph.D.

Lawrence S. Moss, Ph.D.

Chung-chieh Shan, Ph.D.

08/29/2014

Acknowledgements

TODO: Write acks.

TODO: Write dedication.

LATTICE-BASED DATA STRUCTURES FOR DETERMINISTIC PARALLEL AND DISTRIBUTED PROGRAMMING

Lindsey Kuper

TODO: Write abstract.

Contents

CHAPTER 1

Introduction

Parallel programming—that is, writing programs that can take advantage of parallel hardware to go faster—is notoriously difficult. A fundamental reason for this difficulty is that programs can yield inconsistent results, or even crash, due to unpredictable interactions between parallel tasks.

Deterministic-by-construction parallel programming models, though, offer the promise of freedom from subtle, hard-to-reproduce nondeterministic bugs in parallel code. While there are many ways to construct deterministic parallel programs and to verify the determinism of individual programs, only a deterministic-by-construction programming model can provide a *language-level* guarantee of determinism: deterministic programs are the only programs that can be expressed within the model.

A deterministic-by-construction programming model is one that ensures that all programs written using the model have the same *observable behavior* every time they are run. How do we define what is observable about a program's behavior? Certainly, we do *not* wish to preserve behaviors such as running time across multiple runs—ideally, a deterministic-by-construction parallel program will run faster when more parallel resources are available. Moreover, we do not want to count scheduling behavior as observable—in fact, we want to specifically *allow* tasks to be scheduled dynamically and unpredictably, without allowing such *schedule nondeterminism* to affect the observable behavior of a program. Therefore, in this dissertation I will define the observable behavior of a program to be *the value to which the program evaluates*.

LK: In my proposal, I had a footnote here: "We assume that programs have no side effects other than state effects." I think I instead just want to say that we *ignore* other side effects. They can *happen*; it's just that they don't count.

This definition of observable behavior ignores side effects other than *state*. Even so, sharing of state between parallel computations raises the possibility of *race conditions* that allow schedule nondeterminism to be observed in the outcome of a program. For instance, if a computation writes 3 to a shared location while another computation writes 4, then a subsequent third computation that reads and returns the location's contents will nondeterministically return 3 or 4, depending on the order in which the first two computations ran. Therefore, if a parallel programming model is to guarantee determinism by construction, it must necessarily limit sharing of mutable state between parallel tasks in some way.

1.1. The deterministic-by-construction parallel programming landscape

There is long-standing work on deterministic-by-construction parallel programming models that limit sharing of state between tasks. The possibilities include:

- *No-shared-state parallelism.* One classic approach to guaranteeing determinism in a parallel programming model is to allow *no* shared mutable state between tasks, forcing tasks to produce values independently. An example of no-shared-state parallelism is pure functional programming with function-level task parallelism, or *futures*—for instance, in Haskell programs that use the `par` and `pseq` combinators [**29**]. The key characteristic of this style of programming is lack of side effects: because programs don't have side effects, expressions can evaluate simultaneously without affecting the eventual value of the program. Also belonging in this category are parallel programming models based on *pure data parallelism*, such as Data Parallel Haskell [**39, 11**] or the River Trail API for JavaScript [**24**], each of which extend existing languages with *parallel array* data types and (observably) pure operations on them. LK: Does it make sense to say that DPH is observably pure? It does mutate arrays.
- *Data-flow parallelism.* In *Kahn process networks* (KPNs) [**26**], as well as in the more restricted *synchronous data flow* systems [**27**], a network of independent "computing stations" communicate with each other through first-in first-out (FIFO) queues, or *channels*. Reading data out of such a FIFO queue is a *blocking* operation: once an attempt to read has started, a computing station cannot do anything else until the data to be read is available. Each station computes a sequential, monotonic function from the *history* of its input channels (*i.e.*, the input it has received so far) to the history

of its output channels (the output it has produced so far). KPNs are the basis for deterministic stream-processing languages such as StreamIt [**23**].

- *Single-assignment parallelism.* In parallel *single-assignment* languages, "full/empty" bits are associated with memory locations so that they may be written to at most once. Single-assignment locations with blocking read semantics are known as *IVars* [**3**] and are a well-established mechanism for enforcing determinism in parallel settings: they have appeared in Concurrent ML as `SyncVars` [**41**]; in the Intel Concurrent Collections (abbreviated "CnC") system [**9**]; and have even been implemented in hardware in Cray MTA machines [**5**]. Although most of these uses incorporate IVars into already-nondeterministic programming environments, the *monad-par* Haskell library [**30**] uses IVars in a deterministic-by-construction setting, allowing user-created threads to communicate through IVars without requiring the `IO` monad. Rather, operations that read and write IVars must run inside a `Par` monad, thus encapsulating them inside otherwise pure programs, and hence a program in which the only effects are `Par` effects is guaranteed to be deterministic.
- *Imperative disjoint parallelism.* Finally, yet another approach to guaranteeing determinism is to ensure that the state accessed by concurrent threads is *disjoint*.LK: This is the first place I've used the word "concurrent". Should I explain concurrency vs. parallelism in a footnote or something? Is it even a useful distinction in this context? Sophisticated permissions systems and type systems make it possible for imperative programs to mutate state in parallel, while guaranteeing that the same state is not accessed simultaneously by multiple threads. I will refer to this style of programming as *imperative disjoint parallelism*, with Deterministic Parallel Java (DPJ) [**7, 6**] as a prominent example.

The four parallel programming models listed above—no-shared-state parallelism, data-flow parallelism, single-assignment parallelism, and imperative disjoint parallelism—all seem to embody rather different mechanisms for exposing parallelism and for ensuring determinism. If we view these different programming models as a toolkit of unrelated choices, though, it is not clear how to proceed when we want to implement an application with multiple parallelizable components that are best suited to different programming models. For example, suppose we have an application in which we wish to use data-flow pipeline parallelism via FIFO queues, but also disjoint parallel mutation of arrays. It is not obvious how to compose two programming models that each only allow communication through a single type of shared data structure—or, if we do manage to compose them, whether or not the determinism guarantee of the individual models is preserved by their composition. Therefore, we seek a general, broadly-applicable model for deterministic parallel programming that is not tied to a particular data structure.

1.2. Lattice-based, monotonic data structures as a basis for deterministic parallelism

In KPNs and other data-flow models, communication takes place over blocking FIFO queues with ever-increasing *channel histories*, while in IVar-based programming models such as CnC and monad-par, a shared data store of blocking single-assignment memory locations grows monotonically. Hence *monotonic data structures*—data structures to which information can only be added and never removed—emerge as a common theme of guaranteed-deterministic programming models.[1]

In this dissertation, I show that *lattice-based* data structures, or *LVars*, are the foundation for a model of deterministic-by-construction parallel programming that allows a more general form of communication between tasks than previously existing guaranteed-deterministic models allowed. LVars generalize IVars and are so named because the states an LVar can take on are elements of an application-specific *lattice*.[2] This application-specific lattice determines the semantics of the `put` and `get` operations that comprise the interface to LVars (which I will explain in detail in Chapter 2):

- The `put` operation can only change an LVar's state in a way that is *monotonically increasing* with respect to the lattice, because it takes the least upper bound of the current state and the new state.
- The `get` operation allows only limited observations of the state of an LVar. It requires the user to specify a *threshold set* of minimum values that can be read from the LVar, where every two elements in the threshold set must have the lattice's greatest element $\top$ as their least upper bound. A call to

[1] In Chapter 2, I will refine this definition of "monotonic data structures" to mean data structures to which information can only be added and never removed, *and* for which the order in which information is added is not observable.

[2] As I will explain in Chapter 2, what I am calling a "lattice" here really need only be a *bounded join-semilattice* augmented with a greatest element $\top$.

get blocks until the LVar in question reaches a (unique) value in the threshold set, then unblocks and returns that value.

Together, least-upper-bound writes via put and threshold reads via get yield a deterministic-by-construction programming model. That is, a program in which put and get operations on LVars are the only side effects will have the same observable result in spite of parallel execution and schedule nondeterminism. LK: Maybe I don't need the next sentence at all; maybe it's covered by the "organization" bullet points below. As we will see in Chapter 2, no-shared-state parallelism, data-flow parallelism and single-assignment parallelism are all subsumed by the LVars programming model, and as we will see in Chapter 4LK: Maybe refer to a specific section?, imperative disjoint parallelism is compatible with LVars as well.

1.2.1. Generalizing from least-upper-bound writes and threshold reads.

TODO: Say something about Section 2.6, and if there's going to be a proof about the generalized model, mention that.

1.3. Quasi-deterministic and event-driven programming with LVars

The LVars model described above guarantees determinism and supports an unlimited variety of shared data structures: anything viewable as a lattice. However, it is not as general-purpose as one might hope. Consider, for instance, an algorithm for unordered graph traversal. A typical implementation involves a monotonically growing set of "seen nodes"; neighbors of seen nodes are fed back into the set until it reaches a fixed point. Such fixpoint computations are ubiquitous, and would seem to be a perfect match for the LVars model due to their use of monotonicity. But they are not expressible using the threshold get and least-upper-bound put operations described in Section 1.2, nor even with the more general alternatives to get and put described in Section 1.2.1.

The problem is that these computations rely on *negative* information about a monotonic data structure, *i.e.*, on the *absence* of certain writes to the data structure. In a graph traversal, for example, neighboring nodes should only be explored if the current node is *not yet* in the set; a fixpoint is reached only if no new neighbors are found; and, of course, at the end of the computation it must be possible to learn exactly which nodes were reachable (which entails learning that certain nodes were not). In Chapter 3, I describe two extensions to the basic LVars model that make such computations possible:

- First, I extend the model with a primitive operation `freeze` for *freezing* an LVar, which allows its contents to be read immediately and exactly, rather than the blocking threshold read that `get` allows. The `freeze` primitive imposes the following trade-off: once an LVar has been frozen, any further writes that would change its value instead raise an exception; on the other hand, it becomes possible to discover the exact value of the LVar, learning both positive and negative information about it, without blocking. Therefore, LVar programs that use `freeze` are *not* guaranteed to be deterministic, because they could nondeterministically raise an exception depending on how `put` and `freeze` operations are scheduled. However, such programs satisfy *quasi-determinism*: all executions that produce a final value produce the *same* final value.
- Second, I add the ability to attach *event handlers* to an LVar. When an event handler has been registered with an LVar, it invokes a *callback function* to run, asynchronously, whenever events arrive (in the form of monotonic updates to the LVar). Crucially, it is possible to check for *quiescence* of a group of handlers, discovering that no callbacks are currently enabled—a transient, negative property. Since quiescence means that there are no further changes to respond to, it can be used to tell that a fixpoint has been reached.

Of course, since more events could arrive later, there is no way to guarantee that quiescence is permanent—but since the contents of the LVar being written to can only be read through `get` or `freeze` operations anyway, early quiescence poses no risk to determinism or quasi-determinism, respectively. In fact, freezing and quiescence work particularly well together because freezing provides a mechanism by which the programmer can safely "place a bet" that all writes have completed. Hence freezing and handlers make possible fixpoint computations like the graph traversal described above. Moreover, if we can ensure that the freeze does indeed happen after all writes have completed, then we can ensure that the computation is deterministic, and it is possible to enforce this "freeze-last" idiom at the implementation level, as I discuss below (and, in more detail, in Chapter 4LK: Refer to a specific section?).

1.4. The LVish library

To demonstrate the practicality of the LVars programming model, in Chapter 4 I will describe *LVish*,[3] a Haskell library for deterministic and quasi-deterministic programming with LVars.

LVish provides a `Par` monad for encapsulating parallel computation and enables a notion of lightweight, library-level threads to be employed with a custom work-stealing scheduler.[4] LVar computations run inside the `Par` monad, which is indexed by an *effect level*, allowing fine-grained specification of the effects that a given computation is allowed to perform. For instance, since `freeze` introduces quasi-determinism, a computation indexed with a deterministic effect level is not allowed to use `freeze`. Thus, the *static type* of an LVish computation reflects its determinism or quasi-determinism guarantee. Furthermore, if a `freeze` is guaranteed to be the *last* effect that occurs in a computation, then it is impossible for that `freeze` to race with a `put`, ruling out the possibility of a run-time `put`-after-`freeze` exception. LVish exposes a `runParThenFreeze` operation that captures this "freeze-last" idiom and has a deterministic effect level.

LVish also provides a variety of lattice-based data structures (*e.g.*, sets, maps, graphs) that support concurrent insertion, but not deletion, during `Par` computations. In addition to those that LVish provides, users may implement their own lattice-based data structures, and LVish provides tools to facilitate the definition of user-defined LVars. I will describe the proof obligations for data structure implementors and give examples of applications that use user-defined LVars as well as those that the library provides.

In addition to discussing the implementation of the LVish library and introducing the above features with examples, Chapter 4 illustrates LVish through three case studies, drawn from my collaborators' and my experience using the LVish library, all of which make use of handlers and freezing:

[3] Available at `http://hackage.haskell.org/package/lvish`.

[4] The `Par` monad exposed by LVish generalizes the original `Par` monad exposed by the *monad-par* library (`http://hackage.haskell.org/package/monad-par`, described by Marlow *et al.* [**30**]), which allows determinism-preserving communication between threads, but only through IVars, rather than LVars.

- First, I describe using LVish to implement a parallel, pipelined, breadth-first graph traversal that finds the connected component of a graph starting from a given node and maps a (possibly expensive) function f over each node in the connected component of a graph. The idea is that the set of results of applying f to nodes become incrementally available to other computations.
- Second, I describe using LVish to parallelize a control flow analysis (k-CFA) algorithm. The goal of k-CFA is to compute the flow of values to expressions in a program. The k-CFA algorithm proceeds in two phases: first, it explores a graph of *abstract states* of the program; then, it summarizes the results of the first phase. Using LVish, these two phases can be pipelined in a manner similar to the pipelined breadth-first graph traversal described above; moreover, the original graph exploration phase can be internally parallelized. I contrast the LVish implementation with the original sequential implementation and give performance results.
- Third, I describe using LVish to parallelize *PhyBin* [**37**], a bioinformatics application for comparing genealogical histories (phylogenetic trees) that relies heavily on a parallel tree-edit distance algorithm [**45**]. In addition to handlers and freezing, the PhyBin application relies on the ability to perform writes to LVars that are commutative and inflationary with respect to the lattice in question, but *not* idempotent (in contrast to the least-upper-bound writes discussed above, which are idempotent). I argue that these non-idempotent writes, which we call `bump` operations, preserve determinism as long as programs do not use `put` and `bump` on the same LVar, a property that can be statically enforced by the aforementioned effect specification system in LVish. TODO: Revise this; say something about Section 2.6.

1.5. Deterministic threshold queries of distributed data structures

The LVars model is closely related to the concept of *conflict-free replicated data types* (CRDTs) [**43**] for enforcing *eventual consistency* [**48**] of replicated objects in a distributed system. In particular, *state-based* or *convergent* replicated data types, abbreviated as *CvRDTs* [**43, 42**], leverage the mathematical properties of join-semilattices to guarantee that all replicas of an object (for instance, in a distributed database) eventually agree.

Although CvRDTs are provably eventually consistent, queries of CvRDTs (unlike threshold reads of LVars) nevertheless allow inconsistent intermediate states of replicas to be observed. That is, if two replicas of a CvRDT object are updated independently, reads of those replicas may disagree until a (least-upper-bound) *merge* operation takes place.

Taking inspiration from LVar-style threshold reads, in Chapter 5 I show how to extend CvRDTs to support deterministic, *strongly consistent* queries using a mechanism called *threshold queries* (or, seen from another angle, I show how to port threshold reads from a shared-memory setting to a distributed one). The threshold query technique generalizes to any lattice, and hence any CvRDT, and allows deterministic observations to be made of replicated objects before the replicas' states have converged. This work has practical relevance since, while many real distributed database systems allow a mix of eventually consistent and strongly consistent queries, CvRDTs only support the former, and threshold queries extend the CvRDT model to support both.

1.6. Thesis statement, and organization of the rest of this dissertation

With the above background, I can state my thesis:LK: This format ripped off from Josh Dunfield.

> Lattice-based data structures are a general and practical foundation for deterministic and quasi-deterministic parallel and distributed programming.

The rest of this dissertation supports my thesis as follows:

- *Lattice-based data structures*: In Chapter 2, I formally define LVars and use them to define λ_{LVar}, a call-by-value parallel calculus with shared state. In Chapter 3, I extend λ_{LVar} to add support for event handlers and the `freeze` operation, calling the resulting language λ_{LVish}.[5] Appendix B contains runnable versions of λ_{LVar} and λ_{LVish} implemented using the PLT Redex semantics engineering system [**18**] for interactive experimentation.
- *general*: In Chapter 2, I defend the generality of the LVars model by showing how previously existing deterministic parallel programming models can be expressed with LVish. This is possible because

[5] λ_{LVish} is the *LVish calculus* described in Kuper *et al*. [**36**]. In this dissertation, I call it λ_{LVish} to avoid confusion with LVish, the Haskell library I describe in Chapter 4.

the definition of λ_{LVar} is parameterized by the choice of lattice. For example, a lattice of channel histories with a prefix ordering allows LVars to represent FIFO channels that implement a Kahn process network, whereas instantiating λ_{LVar} with a lattice with one "empty" state and multiple "full" states (where $\forall i.\ \mathit{empty} < \mathit{full}_i$) results in a parallel single-assignment language. Hence λ_{LVar} is actually a *family* of calculi, varying by choice of lattice. TODO: Something about Section 2.6 should go here as well.

- *deterministic*: In Chapter 2, I defend the claim that the basic LVars model guarantees determinism by giving a proof of determinism for λ_{LVar}, including the aforementioned `put` and `get` operations on LVars. TODO: If there's a proof to accompany the generalized model in Section 2.6, something about that should go here.
- *quasi-deterministic*: In Chapter 3, I defend this claim by defining quasi-determinism and giving a proof of quasi-determinism for the full λ_{LVish} calculus with the additions of the `freeze` operation and event handlers.
- *practical*: In Chapter 4, I defend the practicality of LVars by describing the LVish Haskell library, which is based on the LVars programming model and demonstrating how it is used for practical programming with the three case studies described above, including performance results.
- *distributed programming*: In Chapter 5, I defend the claim that the LVars programming model is applicable to distributed programming by showing how to extend distributed replicated data structures with LVar-style threshold reads.

1.7. Previously published work

This dissertation draws heavily on the earlier work and writing appearing in the following papers, written jointly with several collaborators:LK: This exact wording stolen from Aaron Turon. maybe tweak it?

- Lindsey Kuper and Ryan R. Newton. 2013. LVars: lattice-based data structures for deterministic parallelism. In *Proceedings of the 2nd ACM SIGPLAN workshop on Functional high-performance computing* (FHPC '13).

- Lindsey Kuper, Aaron Turon, Neelakantan R. Krishnaswami, and Ryan R. Newton. 2014. Freeze after writing: quasi-deterministic parallel programming with LVars. In *Proceedings of the 41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages* (POPL '14).
- Lindsey Kuper, Aaron Todd, Sam Tobin-Hochstadt, and Ryan R. Newton. 2014. Taming the parallel effect zoo: extensible deterministic parallelism with LVish. In *Proceedings of the 35th ACM SIGPLAN Conference on Programming Language Design and Implementation* (PLDI '14).

LK: I was going to have something like, "The material in this chapter is based on research done jointly with..." in individual chapters, and cite the papers there. However, the material in the chapters doesn't exactly correspond to the papers; for instance, the stuff about generalized threshold sets is from the DISC paper, but it's in chapter 2. So I'm just going to try citing all the papers up front.

CHAPTER 2

LVars: lattice-based data structures for deterministic parallelism

Programs written using a *deterministic-by-construction* model of parallel computation are guaranteed to always produce the same observable results, offering programmers freedom from subtle, hard-to-reproduce nondeterministic bugs. While a number of popular languages and language extensions (*e.g.*, Cilk [**21**]LK: Any others?) *encourage* deterministic parallel programming, few of them guarantee determinism at the language level—that is, for *all* programs that can be written using the model.

Of the options available for parallel programming with a language-level determinism guarantee, perhaps the most mature and broadly available choice is pure functional programming with function-level task parallelism, or *futures*. For example, Haskell programs using futures by means of the `par` and `pseq` combinators can provide real speedups on practical programs while guaranteeing determinism [**29**].[1] Yet pure programming with futures is not ideal for all problems. Consider a *producer/consumer* computation in which producers and consumers can be scheduled onto separate processors, each able to keep their working sets in cache. Such a scenario enables *pipeline parallelism* and is common, for instance, in stream processing. But a clear separation of producers and consumers is difficult with futures, because whenever a consumer forces a future, if the future is not yet available, the consumer immediately switches roles to begin computing the value (as explored by Marlow *et al.* [**30**]).

Since pure programming with futures is a poor fit for producer/consumer computations, one might then turn to *stateful* deterministic parallel models. Shared state between computations allows the possibility for race conditions that introduce nondeterminism, so any parallel programming model that hopes to guarantee determinism must do something to tame sharing—that is, to restrict access to mutable state shared among concurrent computations. Systems such as Deterministic Parallel Java [**7, 6**], for instance,

[1] When programming with `par` and `pseq`, a language-level determinism guarantee obtains if user programs are written in the *Safe Haskell* [**46**] subset of Haskell (which is implemented in GHC Haskell by means of the `SafeHaskell` language pragma), and if they do not use the `IO` monad.

accomplish this by ensuring that the state accessed by concurrent threads is *disjoint*. Alternatively, a programming model might allow *data* to be shared, but limit the *operations* that can be performed on it to only those operations that commute with one another and thus can tolerate nondeterministic thread interleavings. In such a setting, although the order in which side-effecting operations occur can differ on multiple runs, a program will always produce the same observable result.[2]

In Kahn process networks (KPNs) [**26**] and other *data-flow parallel* models—which are the basis for deterministic stream-processing languages such as StreamIt [**23**]—communication among processes takes place over blocking FIFO queues with ever-increasing *channel histories*. Meanwhile, in *single-assignment* [**47**] or *IVar-based* [**3**] programming models, such as the Intel Concurrent Collections system (CnC) [**9**] and the *monad-par* Haskell library [**30**], a shared data store of blocking single-assignment memory locations grows monotonically. Hence *monotonic data structures*—data structures to which information can only be added and never removed, and for which the order in which information is added is not observable—emerge as a common theme of both data-flow and single-assignment parallel programming models.

Because state modifications that only add information and never destroy it can be structured to commute with one another and thereby avoid race conditions, it stands to reason that diverse deterministic parallel programming models would leverage the principle of monotonicity. Yet systems like StreamIt, CnC, and monad-par emerge independently, without recognition of their common basis. Moreover, since each one of these programming models is based on a single type of shared data structure, they lack *generality*: IVars or FIFO streams alone cannot support all producer/consumer applications, as I discuss in Section 2.1.

Instead of limiting ourselves to a single type of shared data structure, though, we can take the more general notion of monotonic data structures as the basis for a new deterministic parallel programming model. In this chapter, I show how to generalize IVars to *LVars*, thus named because the states an LVar

[2] There are many ways to define what is observable about a program. As noted in Chapter 1, I define the observable behavior of a program to be the value to which it evaluates.

can take on are elements of an application-specific *lattice*.[3] Section 2.2 introduces the concept of LVars through a series of examples. Then, in Sections 2.3 and 2.4 I formally define λ_{LVar}, a deterministic parallel calculus with shared state, based on the call-by-value λ-calculus. The λ_{LVar} language is general enough to subsume existing deterministic parallel languages because it is parameterized by the choice of lattice. For example, a lattice of channel histories with a prefix ordering allows LVars to represent FIFO channels that implement a Kahn process network, whereas instantiating λ_{LVar} with a lattice with "empty" and "full" states (where $\mathit{empty} < \mathit{full}$) results in a parallel single-assignment language. Different instantiations of the lattice result in a family of deterministic parallel languages.

Because lattices are composable, any number of diverse monotonic data structures can be used together safely. Moreover, as long as a data structure presents the LVar interface, it is fine to use an existing, optimized concurrent data structure implementation; we need not rewrite the world's data structures to leverage the λ_{LVar} determinism result.

The main technical result of this chapter is a proof of determinism for λ_{LVar} (Section 2.5). The key lemma, Independence (Section 2.5.2), gives a kind of *frame property* for LVar computations: very roughly, if a computation takes an LVar from state d to d', then it would take the same LVar from the state $d \sqcup d_F$ to $d' \sqcup d_F$. The Independence lemma captures the commutative effects of LVar computations. Interestingly, such a property would *not* hold in a typical language with shared mutable state, but holds in the setting of λ_{LVar} because of the monotonic semantics of LVars.

Finally, in Section 2.6, TODO: Say something about 2.6 here.

2.1. Motivating example: a parallel, pipelined graph computation

What applications motivate going beyond IVars and FIFO streams? Consider applications in which independent subcomputations contribute information to shared mutable data structures that change monotonically. Hindley-Milner type inference is one example: in a parallel type-inference algorithm, each type variable monotonically acquires information through unification (which can be represented as a

[3] This "lattice" need only be a *bounded join-semilattice* augmented with a greatest element $\top$, in which every two elements have a least upper bound but not necessarily a greatest lower bound; see Section 2.3.1. For brevity, I use the term "lattice" in place of "bounded join-semilattice with a designated greatest element" throughout this dissertation.

lattice). Likewise, in control-flow analysis, the *set* of locations to which a variable refers monotonically *shrinks*. In logic programming, a parallel implementation of conjunction might asynchronously add information to a logic variable from different threads.

To illustrate the issues that arise in computations of this nature, consider a specific problem, drawn from the domain of *graph algorithms*, where issues of ordering create a tension between parallelism and determinism:

> In a directed graph, find the connected component containing a vertex v, and compute a (possibly expensive) function f over all vertices in that component, making the set of results available asynchronously to other computations.

For example, in a directed graph representing user profiles on a social network and the connections between them, where v represents a particular profile, we might wish to find all (or the first k degrees of) profiles connected to v, then map a function f over each profile in that set in parallel.

This is a challenge problem for deterministic-by-construction parallel programming: existing parallel solutions (such as, for instance, the parallel breadth-first graph traversal implementation from the Parallel Boost Graph Library [**1**]) often traverse the connected component in a nondeterministic order (even though the outcome of the program—that is, the final connected component—is deterministic), and IVars and streams provide no obvious aid. For example, IVars cannot accumulate sets of visited nodes, nor can they be used as "mark bits" on visited nodes, since they can only be written once and not tested for emptiness. Streams, on the other hand, impose an excessively strict ordering for computing the unordered *set* of vertex labels in a connected component. Before turning to an LVar-based approach, though, let's consider whether a purely functional (and therefore deterministic by construction) program can meet the specification.

2.1.1. A purely functional attempt. Figure 2.1 gives a Haskell implementation of a *level-synchronized* breadth-first graph traversal that finds the connected component reachable from a starting vertex. Nodes at distance one from the starting vertex are discovered—and set-unioned into the connected component—before nodes of distance two are considered. Level-synchronization is a popular strategy for parallel breadth-first graph traversal (in fact, the aforementioned implementation from the Parallel Boost

```
nbrs :: Graph → NodeLabel → Set NodeLabel
-- `nbrs g n' is the neighbor nodes of node `n' in graph `g'.

-- Traverse each level of the graph in parallel, maintaining at each
-- recursive step a set of nodes that have been seen and a set of
-- nodes left to process.
bf_traverse :: Graph → Set NodeLabel → Set NodeLabel → Set NodeLabel
bf_traverse g seen nu =
  if nu == {}
  then seen
  else let seen'  = union seen nu
           allNbr = parFold union (parMap (nbrs g) nu)
           nu'    = difference allNbr seen'
       in bf_traverse g seen' nu'

-- Next we traverse the connected component, starting with the vertex
-- `profile0':
ccmp = bf_traverse profiles {} {profile0}
result = parMap analyze ccmp
```

Figure 2.1. A purely functional Haskell program that maps the analyze function over the connected component of the profiles graph that is reachable from the node profile0. Although component discovery proceeds in parallel, results of analyze are not asynchronously available to other computations, inhibiting pipelining.

Graph Library [**1**] uses level-synchronization), although it necessarily sacrifices some parallelism for determinism: parallel tasks cannot continue discovering nodes in the component before synchronizing with all other tasks at a given distance from the start.

Unfortunately, the code given in Figure 2.1 does not quite implement the problem specification given above. Even though connected-component discovery is parallel, members of the output set do not become available to other computations until component discovery is *finished*, limiting parallelism. We could manually push the `analyze` invocation inside the `bf_traverse` function, allowing the `analyze` computation to start sooner, but doing so just passes the problem to the downstream consumer, unless we are able to perform a heroic whole-program fusion.

If `bf_traverse` returned a list, lazy evaluation could make it possible to *stream* results to consumers incrementally. But since it instead returns a *set*, such pipelining is not generally possible: consuming the results early would create a proof obligation that the determinism of the consumer does not depend on the order in which results emerge from the producer.[4]

A compromise would be for `bf_traverse` to return a list of "level-sets": distance one nodes, distance two nodes, and so on. Thus level-one results could be consumed before level-two results are ready. Still, at the granularity of the individual level-sets, the problem would remain: within each level-set, one would not be able to launch all instances of `analyze` and asynchronously use those results that finished first. Moreover, we would still have to contend with the previously-mentioned difficulty of separating producers and consumers when expressing producer-consumer computations when using pure programming with futures [**30**].

2.1.2. An LVar-based solution. Consider a version of `bf_traverse` written using a programming model with limited effects that allows *any* data structure to be shared among tasks, including sets and graphs, so long as that data structure grows monotonically. Consumers of the data structure may execute as soon as data is available, enabling pipelining, but may only observe irrevocable, monotonic properties of it. This is possible with a programming model based on LVars. In the rest of this chapter, I will formally introduce LVars and the λ_{LVar} language and give a proof of determinism for λ_{LVar}. Then, in Chapter 3, I will extend the basic LVars model with additional features that make it easier to implement parallel graph traversal algorithms and other fixpoint computations, and I will return to `bf_traverse`

[4] As intuition for this idea, consider that purely functional set data structures, such as Haskell's `Data.Set`, are typically represented with balanced trees. Unlike with lists, the structure of the tree is not known until all elements are present.

and show how to implement a version of it using LVars that makes pipelining possible and truly satisfies the above specification.

2.2. LVars by example

IVars [**3, 38, 9, 30**] are a well-known mechanism for deterministic parallel programming. An IVar is a *single-assignment* variable [**47**] with a blocking read semantics: an attempt to read an empty IVar will block until the IVar has been filled with a value. LVars are a generalization of IVars: unlike IVars, which can only be written to once, LVars allow multiple writes, so long as those writes are monotonically increasing with respect to an application-specific lattice of states.

Consider a program (written in a hypothetical language) in which two parallel computations write to an LVar *lv*, with one thread writing the value 2 and the other writing 3:

(Example 2.1)

$$\begin{array}{l} \texttt{let par}\ \_ = \texttt{put}\ \mathit{lv}\ 3 \\ \qquad\quad\ \ \_ = \texttt{put}\ \mathit{lv}\ 2 \\ \ \ \texttt{in get}\ \mathit{lv} \end{array}$$

Here, put and get are operations that write and read LVars, respectively, and the expression

$$\texttt{let par}\ x_1 = e_1;\ x_2 = e_2;\ \ldots\ \texttt{in}\ \mathit{body}$$

has *fork-join* semantics: it launches concurrent subcomputations $e_1, e_2, \ldots$ whose executions arbitrarily interleave, but must all complete before *body* runs. The put operation is defined in terms of the application-specific lattice of LVar states: it updates the LVar to the *least upper bound* of its current state and the new state being written.

If *lv*'s lattice is the $\leq$ ordering on positive integers, as shown in Figure 2.2(a), then *lv*'s state will always be max$(3, 2) = 3$ by the time get *lv* runs, since the least upper bound of two positive integers n_1 and n_2 is max(n_1, n_2). Therefore Example 2.1 will deterministically evaluate to 3, regardless of the order in which the two put operations occurred.

On the other hand, if *lv*'s lattice is that shown in Figure 2.2(b), in which the least upper bound of any two distinct positive integers is $\top$, then Example 2.1 will deterministically raise an exception, indicating that conflicting writes to *lv* have occurred. This exception is analogous to the "multiple put" error raised

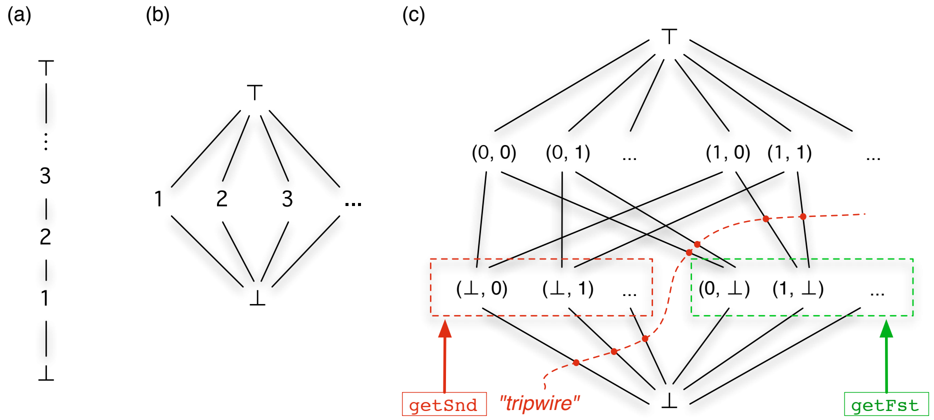


Figure 2.2. Example LVar lattices: (a) positive integers ordered by $\leq$; (b) IVar containing a positive integer; (c) pair of natural-number-valued IVars, annotated with example threshold sets that would correspond to a blocking read of the first or second element of the pair. Any state transition crossing the "tripwire" for `getSnd` causes it to unblock and return a result.

upon multiple writes to an IVar. Unlike with a traditional IVar, though, multiple writes of the *same* value (say, put *lv* 3 and put *lv* 3) will *not* raise an exception, because the least upper bound of any positive integer and itself is that integer—corresponding to the fact that multiple writes of the same value do not allow any nondeterminism to be observed.

2.2.1. Threshold reads. However, merely ensuring that writes to an LVar are monotonically increasing is not enough to ensure that programs behave deterministically. Consider again the lattice of Figure 2.2(a) for *lv*, but suppose we change Example 2.1 to allow the get operation to be interleaved with the two puts:

(Example 2.2)

$$\begin{array}{l} \texttt{let par}\ \_ = \texttt{put}\ \mathit{lv}\ 3 \\ \qquad\quad\ \ \_ = \texttt{put}\ \mathit{lv}\ 2 \\ \qquad\quad\ \ x = \texttt{get}\ \mathit{lv} \\ \ \ \texttt{in}\ x \end{array}$$

Since the two puts and the get can be scheduled in any order, Example 2.2 is nondeterministic: x might be either 2 or 3, depending on the order in which the LVar effects occur. Therefore, to maintain determinism, LVars put an extra restriction on the get operation. Rather than allowing get to observe the exact value of the LVar, it can only observe that the LVar has reached one of a specified set of *lower bound* states. This set of lower bounds, which we provide as an extra argument to get, is called a *threshold set* because the values in it form a "threshold" that the state of the LVar must cross before the call to get is allowed to unblock and return. When the threshold has been reached, get unblocks and returns *not* the exact value of the LVar, but instead, the (unique) element of the threshold set that has been reached or surpassed.

We can make Example 2.2 behave deterministically by passing a threshold set argument to get:

(Example 2.3)

```
let par _ = put lv 3
        _ = put lv 2
        x = get lv {3}
 in x
```

For instance, suppose we choose the singleton set $\{3\}$ as the threshold set. Since *lv*'s value can only increase with time, we know that once it is at least 3, it will remain at or above 3 forever; therefore the program will deterministically evaluate to 3. Had we chosen $\{2\}$ as the threshold set, the program would deterministically evaluate to 2; had we chosen $\{4\}$, it would deterministically block forever.

As long as we only access LVars with put and (thresholded) get, we can arbitrarily share them between threads without introducing nondeterminism. That is, the put and get operations in a given program can happen in any order, without changing the value to which the program evaluates.

2.2.2. Incompatibility of threshold sets. While the LVar interface just described is deterministic, it is only useful for synchronization, not for communicating data: we must specify in advance the single answer we expect to be returned from the call to get. In general, though, threshold sets do not have to be singleton sets. For example, consider an LVar *lv* whose states form a lattice of *pairs* of natural-number-valued IVars; that is, *lv* is a pair (m, n), where m and n both start as $\bot$ and may each be updated once with a non-$\bot$ value, which must be some natural number. This lattice is shown in Figure 2.2(c).

We can then define `getFst` and `getSnd` operations for reading from the first and second entries of *lv*:

$$\texttt{getFst}\, p \overset{\triangle}{=} \texttt{get}\, p\, \{(m, \bot) \mid m \in \mathbb{N}\}$$
$$\texttt{getSnd}\, p \overset{\triangle}{=} \texttt{get}\, p\, \{(\bot, n) \mid n \in \mathbb{N}\}$$

This allows us to write programs like the following:

$$\begin{array}{ll} & \texttt{let par}\ \_ = \texttt{put}\ \mathit{lv}\ (\bot, 4) \\ \text{(Example 2.4)} & \qquad\qquad \_ = \texttt{put}\ \mathit{lv}\ (3, \bot) \\ & \qquad\qquad x = \texttt{getSnd}\ \mathit{lv} \\ & \ \ \texttt{in}\ x \end{array}$$

In the call `getSnd` *lv*, the threshold set is $\{(\bot, 0), (\bot, 1), \dots\}$, an infinite set. There is no risk of nondeterminism because the elements of the threshold set are *pairwise incompatible* with respect to *lv*'s lattice: informally, since the second entry of *lv* can only be written once, no more than one state from the set $\{(\bot, 0), (\bot, 1), \dots\}$ can ever be reached. (I formalize this incompatibility requirement in Section 2.3.3.)

In the case of Example 2.4, `getSnd` *lv* may unblock and return $(\bot, 4)$ any time after the second entry of *lv* has been written, regardless of whether the first entry has been written yet. It is therefore possible to use LVars to safely read parts of an incomplete data structure—say, an object that is in the process of being initialized by a constructor.

2.2.3. The model versus reality. The use of explicit threshold sets in the above LVars model should be understood as a mathematical modeling technique, *not* an implementation approach or practical API. The LVish library (which I will discuss in Chapter 4) provides an unsafe `getLV` operation to the authors of LVar data structure libraries, who can then make operations like `getFst` and `getSnd` available as a safe interface for application writers, implicitly baking in the particular threshold sets that make sense for a given data structure without ever explicitly constructing them.

To put it another way, operations on a data structure exposed as an LVar must have the *semantic effect* of a least upper bound for writes or a threshold for reads, but none of this need be visible to clients (or even written explicitly in the code). Any data structure API that provides such a semantics is guaranteed to provide deterministic concurrent communication.

2.3. Lattices, stores, and determinism

As a minimal substrate for LVars, I introduce λ_{LVar}, a parallel call-by-value λ-calculus extended with a *store* and with communication primitives `put` and `get` that operate on data in the store. The class of programs that I am interested in modeling with λ_{LVar} are those with explicit effectful operations on shared data structures, in which parallel subcomputations may communicate with each other via the `put` and `get` operations.

In this setting of shared mutable state, the trick that λ_{LVar} employs to maintain determinism is that stores contain *LVars*, which are a generalization of IVars.[5] Whereas IVars are single-assignment variables—either empty or filled with an immutable value—an LVar may have an arbitrary number of states forming a set D, which is partially ordered by a relation $\sqsubseteq$. An LVar can take on any sequence of states from D, so long as that sequence respects the partial order—that is, so long as updates to the LVar (made via the `put` operation) are *inflationary* with respect to $\sqsubseteq$. Moreover, the `get` operation allows only limited observations of the LVar's state. In this section, I discuss how lattices and stores work in λ_{LVar} and explain how the semantics of `put` and `get` together enforce determinism in λ_{LVar} programs.

2.3.1. Lattices. The definition of λ_{LVar} is parameterized by D: to write concrete λ_{LVar} programs, we must specify the set of LVar states that we are interested in working with, and an ordering on those states. Therefore λ_{LVar} is actually a *family* of languages, rather than a single language.

Formally, D is a *bounded join-semilattice* augmented with a greatest element $\top$. That is, D has the following structure:

- D has a least element $\bot$, representing the initial "empty" state of an LVar.
- D has a greatest element $\top$, representing the "error" state that results from conflicting updates to an LVar.

[5] IVars are so named because they are a special case of *I-structures* [3]—namely, those with only one cell.

- D comes equipped with a partial order $\sqsubseteq$, where $\bot \sqsubseteq d \sqsubseteq \top$ for all $d \in D$.
- Every pair of elements in D has a least upper bound (lub), written $\sqcup$. Intuitively, the existence of a lub for every two elements in D means that it is possible for two subcomputations to independently update an LVar, and then deterministically merge the results by taking the lub of the resulting two states.

We can specify all these components as a 4-tuple $(D, \sqsubseteq, \bot, \top)$ where D is a set, $\sqsubseteq$ is a partial order on the elements of D, $\bot$ is the least element of D according to $\sqsubseteq$, and $\top$ is the greatest. However, I use D as a shorthand for the entire 4-tuple $(D, \sqsubseteq, \bot, \top)$ when its meaning is clear from the context.

Virtually any data structure to which information is added gradually can be represented as a lattice, including pairs, arrays, trees, maps, and infinite streams. In the case of maps or sets, $\sqcup$ could be defined as union; for pointer-based data structures like tries, it could allow for unification of partially-initialized structures.

LK: Since I've already talked abut this stuff in Section 2.2, I'm kind of worried that having it here again belabors the point, although the treatment here is more formal.

The simplest example of a useful lattice is one that represents the states that a a single-assignment variable (that is, an IVar) can take on. A natural-number-valued IVar, for instance, has a state space corresponding to the lattice in Figure 2.2(b), that is,

$$D = (\{\top, \bot\} \cup \mathbb{N}, \sqsubseteq, \bot, \top),$$

where the partial order $\sqsubseteq$ is defined by setting $\bot \sqsubseteq d \sqsubseteq \top$ and $d \sqsubseteq d$ for all $d \in D$. This is a lattice of height three and infinite width, where the naturals are arranged horizontally. After the initial write of some $n \in \mathbb{N}$, any further conflicting writes would push the state of the IVar to $\top$ (an error). For instance, if one thread writes 2 and another writes 1 to an IVar (in arbitrary order), the second of the two writes would result in an error because $2 \sqcup 1 = \top$.

In the lattice of Figure 2.2(a), on the other hand, the $\top$ state is unreachable, because the least upper bound of any two writes is just the maximum of the two. If one thread writes 2 and another writes 1, the resulting state will be 2, since $2 \sqcup 1 = 2$. Here, the unreachability of $\top$ models the fact that no conflicting updates can occur to the LVar.

2.3.2. Stores. During the evaluation of a λ_{LVar} program, a *store* S keeps track of the states of LVars. Each LVar is represented by a binding from a location l, drawn from a set *Loc*, to its state, which is some element $d \in D$. Although each LVar in a program has its own state, the states of all the LVars are drawn from the same lattice D. We can do this with no loss of generality because lattices corresponding to different types of LVars could always be unioned into a single lattice (with shared $\top$ and $\bot$ elements).[6]

Definition 2.1. A *store* is either a finite partial mapping $S : \mathit{Loc} \overset{\text{fin}}{\rightarrow} (D - \{\top\})$, or the distinguished element $\top_S$.

I use the notation $S[l \mapsto d]$ to denote extending S with a binding from l to d. If $l \in \mathit{dom}(S)$, then $S[l \mapsto d]$ denotes an update to the existing binding for l, rather than an extension. Another way to denote a store is by explicitly writing out all its bindings, using the notation $[l_1 \mapsto d_1, \ldots, l_n \mapsto d_n]$. The state space of stores forms a bounded join-semilattice augmented with a greatest element, just as D does, with the empty store $\bot_S$ as its least element and $\top_S$ as its greatest element. It is straightforward to lift the $\sqsubseteq$ and $\sqcup$ operations defined on elements of D to the level of stores:

Definition 2.2. A store S is *less than or equal to* a store S' (written $S \sqsubseteq_S S'$) iff:

- $S' = \top_S$, or
- $\mathit{dom}(S) \subseteq \mathit{dom}(S')$ and for all $l \in \mathit{dom}(S)$, $S(l) \sqsubseteq S'(l)$.

Definition 2.3. The *least upper bound (lub)* of two stores S_1 and S_2 (written $S_1 \sqcup_S S_2$) is defined as follows:

- $S_1 \sqcup_S S_2 = \top_S$ iff there exists some $l \in \mathit{dom}(S_1) \cap \mathit{dom}(S_2)$ such that $S_1(l) \sqcup S_2(l) = \top$.
- Otherwise, $S_1 \sqcup_S S_2$ is the store S such that:
  - $\mathit{dom}(S) = \mathit{dom}(S_1) \cup \mathit{dom}(S_2)$, and
  - For all $l \in \mathit{dom}(S)$:

$$S(l) = \begin{cases} S_1(l) \sqcup S_2(l) & \text{if } l \in \mathit{dom}(S_1) \cap \mathit{dom}(S_2) \\ S_1(l) & \text{if } l \notin \mathit{dom}(S_2) \\ S_2(l) & \text{if } l \notin \mathit{dom}(S_1) \end{cases}$$

[6] Alternatively, in a typed formulation of λ_{LVar}, the type of an LVar might determine the lattice of its states.

Equivalence of stores is also straightforward. Two stores are equal if they are both $\top_S$ or if they both have the same set of bindings:

Definition 2.4. Two stores S and S' are *equal* iff:

(1) $S = \top_S$ and $S' = \top_S$, or
(2) $dom(S) = dom(S')$ and for all $l \in dom(S)$, $S(l) = S'(l)$.

By Definition 2.3, if $d_1 \sqcup d_2 = \top$, then $[l \mapsto d_1] \sqcup_S [l \mapsto d_2] = \top_S$. Notice that a store containing a binding $l \mapsto \top$ can never arise during the execution of a λ_{LVar} program, because (as I will show in Section 2.4) an attempted write that would take the state of l to $\top$ would raise an error before the write can occur.

2.3.3. Communication primitives. The `new`, `put`, and `get` operations create, write to, and read from LVars, respectively. The interface is similar to that presented by mutable references:

- `new` extends the store with a binding for a new LVar whose initial state is $\bot$, and returns the location l of that LVar (*i.e.*, a pointer to the LVar).
- `put` takes a pointer to an LVar and a new state and updates the LVar's state to the *least upper bound* of the current state and the new state, potentially pushing the state of the LVar upward in the lattice. Any update that would take the state of an LVar to $\top$ results in an error.
- `get` performs a blocking "threshold" read that allows limited observations of the state of an LVar. It takes a pointer to an LVar and a *threshold set* T, which is a non-empty subset of D that is *pairwise incompatible*, meaning that the lub of any two distinct elements in T is $\top$. If the LVar's state d_1 in the lattice is *at or above* some $d_2 \in T$, the `get` operation unblocks and returns d_2. Note that d_2 is a unique element of T, for if there is another $d_2' \neq d_2$ in the threshold set such that $d_2' \sqsubseteq d_1$, it would follow that $d_2 \sqcup d_2' \sqsubseteq d_1$, and so $d_2 \sqcup d_2'$ cannot be $\top$, which contradicts the requirement that T be pairwise incompatible.

The intuition behind `get` is that it specifies a subset of the lattice that is "horizontal": no two elements in the threshold set can be above or below one another. Intuitively, each element in the threshold set is an "alarm" that detects the activation of itself or any state above it. One way of visualizing the threshold set for a get operation is as a subset of edges in the lattice that, if crossed, set off the corresponding alarm. Together these edges form a "tripwire". Figure 2.2(b) shows what the "tripwire" looks like for an example get operation. The threshold set $\{(\bot, 0), (\bot, 1), ...\}$ (or a subset thereof) would pass the incompatibility test, as would the threshold set $\{(0, \bot), (1, \bot), ...\}$ (or a subset thereof), but a combination of the two would not pass.

The requirement that the elements of a threshold set be pairwise incompatible limits the expressivity of threshold sets. In fact, it is a stronger requirement than we need to ensure determinism. Later on, in Section 2.6, I will explain how to generalize the definition of a threshold set to make more programs expressible. For now, I will proceed with the simpler definition above.

2.3.4. Monotonic store growth and determinism. In IVar-based languages, a store can only change in one of two ways: a new, empty location (pointing to $\bot$) is created, or a previously $\bot$ binding is permanently updated to a meaningful value. It is therefore straightforward in such languages to define an ordering on stores and establish determinism based on the fact that stores grow monotonically with respect to the ordering. For instance, *Featherweight CnC* [**9**], a single-assignment imperative calculus that models the Intel Concurrent Collections (CnC) system, defines ordering on stores as follows:[7]

Definition 2.5 (store ordering, Featherweight CnC). A store S is *less than or equal to* a store S' (written $S \sqsubseteq_S S'$) iff $\mathit{dom}(S) \subseteq \mathit{dom}(S')$ and for all $l \in \mathit{dom}(S)$, $S(l) = S'(l)$.

Our Definition 2.2 is reminiscent of Definition 2.5, but Definition 2.5 requires that $S(l)$ and $S'(l)$ be *equal*, instead of our weaker requirement that $S(l)$ be *less than or equal to* $S'(l)$ according to the application-specific lattice $\sqsubseteq$. In λ_{LVar}, stores may grow by updating existing bindings via repeated puts, so Definition 2.5 would be too strong; for instance, if $\bot \sqsubset d_1 \sqsubseteq d_2$ for distinct $d_1, d_2 \in D$, the relationship $[l \mapsto (d_1,)] \sqsubseteq_S [l \mapsto (d_2,)]$ holds under Definition 2.2, but would not hold under Definition 2.5. That is, in λ_{LVar} an LVar could take on the state d_1 followed by d_2, which would not be possible in Featherweight CnC.

[7] A minor difference between λ_{LVar} and Featherweight CnC is that, in Featherweight CnC, no store location is explicitly bound to $\bot$. Instead, if $l \notin \mathit{dom}(S)$, then l is defined to point to $\bot$.

Given a lattice $(D, \sqsubseteq, \bot, \top)$ with elements $d \in D$:

$$\begin{array}{rrcl}
\text{configurations} & \sigma & ::= & \langle S;\, e\rangle \mid \textbf{error} \\
\text{expressions} & e & ::= & x \mid v \mid e\, e \mid \texttt{get}\; e\, e \mid \texttt{put}\; e\, e \mid \texttt{new} \\
\text{values} & v & ::= & \texttt{()} \mid d \mid l \mid T \mid \lambda x.\, e \\
\text{threshold sets} & T & ::= & \{d_1,\, d_2,\, \ldots\} \\
\text{stores} & S & ::= & [l_1 \mapsto d_1,\, \ldots,\, l_n \mapsto d_n] \mid \top_S \\
\text{evaluation contexts} & E & ::= & [\,] \mid E\, e \mid e\, E \mid \texttt{get}\; E\, e \mid \texttt{get}\; e\, E \mid \texttt{put}\; E\, e \mid \texttt{put}\; e\, E
\end{array}$$

Figure 2.3. Syntax for λ_{LVar}.

Given a lattice $(D, \sqsubseteq, \bot, \top)$ with elements $d \in D$:

$$\mathit{incomp}(T) \triangleq \forall\, d_1, d_2 \in T.\, (d_1 \neq d_2 \implies d_1 \sqcup d_2 = \top) \qquad \boxed{\sigma \hookrightarrow \sigma'}$$

E-Eval-Ctxt
$$\frac{\langle S;\, e\rangle \hookrightarrow \langle S';\, e'\rangle}{\langle S;\, E[e]\rangle \hookrightarrow \langle S';\, E[e']\rangle}$$

E-Beta
$$\frac{}{\langle S;\, (\lambda x.\, e)\, v\rangle \hookrightarrow \langle S;\, e[x := v]\rangle}$$

E-New
$$\frac{}{\langle S;\, \texttt{new}\rangle \hookrightarrow \langle S[l \mapsto \bot];\, l\rangle}\ (l \notin \mathit{dom}(S))$$

E-Put
$$\frac{S(l) = d_1 \qquad d_1 \sqcup d_2 \neq \top}{\langle S;\, \texttt{put}\; l\; d_2\rangle \hookrightarrow \langle S[l \mapsto d_1 \sqcup d_2];\, \texttt{()}\rangle}$$

E-Put-Err
$$\frac{S(l) = d_1 \qquad d_1 \sqcup d_2 = \top}{\langle S;\, \texttt{put}\; l\; d_2\rangle \hookrightarrow \textbf{error}}$$

E-Get
$$\frac{S(l) = d_1 \qquad \mathit{incomp}(T) \qquad d_2 \in T \qquad d_2 \sqsubseteq d_1}{\langle S;\, \texttt{get}\; l\; T\rangle \hookrightarrow \langle S;\, d_2\rangle}$$

Figure 2.4. An operational semantics for λ_{LVar}.

I establish in Section 2.5 that λ_{LVar} remains deterministic despite the relatively weak $\sqsubseteq_S$ relation given in Definition 2.2. The keys to maintaining determinism are the blocking semantics of the `get` operation and the fact that it allows only *limited* observations of the state of an LVar.

2.4. λ_{LVar}: syntax and semantics

LK: Maybe this should be explained more slowly—that is, maybe I should individually go through each thing in the grammar and say what it is. I wouldn't do that in a conference paper, but...this isn't a conference paper.

The syntax and operational semantics of λ_{LVar} appear in Figures 2.3 and 2.4, respectively. Both the syntax and semantics are parameterized by the lattice $(D, \sqsubseteq, \bot, \top)$. The reduction relation $\hookrightarrow$ is defined on *configurations* $\langle S;\ e \rangle$ comprising a store and an expression. The *error configuration*, written **error**, is a unique element added to the set of configurations, but $\langle \top_S;\ e \rangle$ is equal to **error** for all expressions e. The metavariable σ ranges over configurations.

λ_{LVar} uses a reduction semantics based on *evaluation contexts*. The E-Eval-Ctxt rule is a standard context rule, allowing reductions to apply within a context. The choice of context determines where evaluation can occur; in λ_{LVar}, the order of evaluation is nondeterministic (that is, a given expression can generally reduce in more than one way), and so it is generally *not* the case that an expression has a unique decomposition into redex and context. For example, in an application $e_1\ e_2$, either e_1 or e_2 might reduce first. The nondeterminism in choice of evaluation context reflects the nondeterminism of scheduling between concurrent threads, and in λ_{LVar}, the arguments to `get`, `put`, and application expressions are *implicitly* evaluated concurrently.

The rules E-New, E-Put/E-Put-Err, and E-Get respectively express the semantics of the `new`, `put`, and `get` operations described in Section 2.3.3. The E-New rule creates a new binding in the store and returns a pointer to it; the side condition $l \notin \mathit{dom}(S)$ ensures that l is a fresh location. The E-Put rule updates the store and returns `()`, the unit value. The E-Put-Err rule applies when a `put` to a location would take its state to $\top$; in that case, the semantics steps to **error**. The incompatibility of the threshold set argument to `get` is enforced in the E-Get rule by the $\mathit{incomp}(T)$ premise, which requires that the least upper bound of any two distinct elements in T must be $\top$.

2.4.1. Fork-join parallelism. λ_{LVar} has a call-by-value semantics: arguments must be fully evaluated before function application (β-reduction, modeled by the E-Beta rule) can occur. I exploit this property to define a syntactic sugar `let par` for *parallel composition*, which computes two subexpressions e_1 and

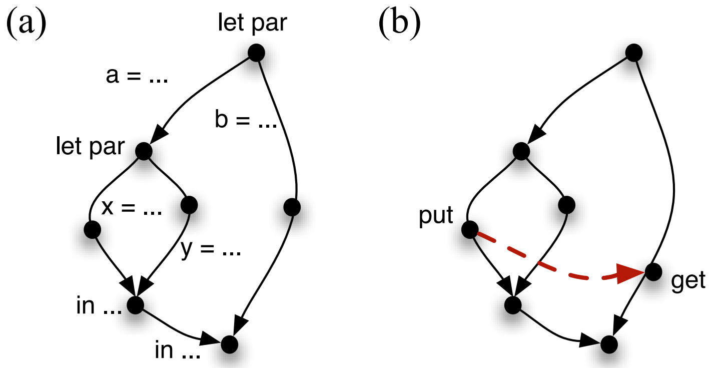


Figure 2.5. A series-parallel graph induced by parallel λ-calculus evaluation (a); a non-series-parallel graph induced by put/get operations (b).

e_2 in parallel before computing e_3:

$$\begin{array}{lcl} \texttt{let par}\ x = e_1 & & \\ \qquad\quad y = e_2 & \triangleq & ((\lambda x.\,(\lambda y.\,e_3))\ e_1)\ e_2 \\ \ \ \texttt{in}\ e_3 & & \end{array}$$

Although e_1 and e_2 can be evaluated in parallel, e_3 cannot be evaluated until both e_1 and e_2 are values, because the call-by-value semantics does not allow β-reduction until the operand is fully evaluated, and because it further disallows reduction under λ-terms (sometimes called "full β-reduction"). In the terminology of parallel programming, a let par expression executes both a *fork* and a *join*. Indeed, it is common for fork and join to be combined in a single language construct, for example, in languages with parallel tuple expressions such as Manticore [**19**].

Since let par expresses *fork-join* parallelism, the evaluation of a program comprising nested let par expressions would induce a runtime dependence graph like that pictured in Figure 2.5(a). The λ_{LVar} language (minus put and get) can support any *series-parallel* dependence graph. Adding communication through put and get introduces "lateral" edges between branches of a parallel computation, as in Figure 2.5(b). This adds the ability to construct arbitrary non-series-parallel dependency graphs, just as with *first-class futures* [**44**].

Because the λ_{LVar} semantics does not reduce under λ-terms, we can sequentially compose e_1 before e_2 by writing `let _ =` e_1 `in` e_2, which desugars to $(\lambda\_.\, e_2)\ e_1$. Sequential composition is useful for, for instance, allocating a new LVar before beginning a sequence of side-effecting `put` and `get` operations on it.

2.5. Proof of determinism for λ_{LVar}

The main technical result of this chapter is a proof of determinism for the λ_{LVar} language. The determinism theorem says that if two executions starting from a given configuration σ terminate in configurations σ' and σ'', then σ' and σ'' are the same configuration, up to a permutation on locations.

In order to prove determinism for λ_{LVar}, I first prove several supporting lemmas. The structure of the proof is similar to that of the proof of determinism for Featherweight CnC given by Budimlić *et al.* [**9**]. I reuse the naming conventions of Budimlić *et al.* for Lemmas 2.1 through 2.5, although the statements and proofs of those lemmas differ considerably in the setting of λ_{LVar}, due to the generality of LVars.

However, Lemmas 2.6 through 2.8 are nearly identical to the corresponding lemmas in the Featherweight CnC determinism proof. This is the case because, once Lemmas 2.1 through 2.5 are established, the remainder of the determinism proof does not need to deal specifically with the semantics of LVars, lattices, or the store, and instead deals only with execution steps at a high level.

TODO: Say something about how later I'll show determinism for generalized monotonic writes and generalized threshold reads, if in fact I'm going to do that.

2.5.1. Monotonicity lemma. The Monotonicity lemma says that, as evaluation proceeds according to the $\hookrightarrow$ relation, the store can only grow with respect to the $\sqsubseteq_S$ ordering.

Lemma 2.1 (Monotonicity). *If* $\langle S;\ e\rangle \hookrightarrow \langle S';\ e'\rangle$*, then* $S \sqsubseteq_S S'$.

Proof. By induction on the derivation of $\langle S;\ e\rangle \hookrightarrow \langle S';\ e'\rangle$, by cases on the last rule in the derivation; see Section A.1. □

2.5.2. Independence lemma.

The Independence lemma establishes a "frame property" for λ_{LVar} that captures the idea that independent effects commute with each other. Consider an expression e that runs starting in store S and steps to e', updating the store to S'. The Independence lemma provides a double-edged guarantee about what will happen if we evaluate e starting from a larger store $S \sqcup_S S''$: first, e will update the store to $S' \sqcup_S S''$; second, e will step to e' as it did before. Here $S \sqcup_S S''$ is the least upper bound of the original S and some other store S'' that is "framed on" to S; intuitively, S'' is the store resulting from some other independently-running computation.

Lemma 2.2 requires as a precondition that the store S'' must be *non-conflicting* with the original transition from $\langle S;\, e\rangle$ to $\langle S';\, e'\rangle$, meaning that locations in S'' cannot share names with locations newly allocated during the transition; this rules out location name conflicts caused by allocation.

Definition 2.6. A store S'' is *non-conflicting* with the transition $\langle S;\, e\rangle \hookrightarrow \langle S';\, e'\rangle$ iff $(\mathit{dom}(S') - \mathit{dom}(S)) \cap \mathit{dom}(S'') = \emptyset$.

Lemma 2.2 (Independence). *If $\langle S;\, e\rangle \hookrightarrow \langle S';\, e'\rangle$ (where $\langle S';\, e'\rangle \neq$ **error**), then for all S'' such that S'' is non-conflicting with $\langle S;\, e\rangle \hookrightarrow \langle S';\, e'\rangle$ and $S' \sqcup_S S'' \neq \top_S$:*

$\langle S \sqcup_S S'';\, e\rangle \hookrightarrow \langle S' \sqcup_S S'';\, e'\rangle$.

Proof. By induction on the derivation of $\langle S;\, e\rangle \hookrightarrow \langle S';\, e'\rangle$, by cases on the last rule in the derivation; see Section A.2. □

2.5.3. Clash lemma.

The Clash lemma, Lemma 2.3, is similar to the Independence lemma, but handles the case where $S' \sqcup_S S'' = \top_S$. It establishes that, in that case, $\langle S \sqcup_S S'';\, e\rangle$ steps to **error**.

LK: We didn't need the Clash lemma for the quasi-determinism proof, but I'm pretty sure the only reason we didn't need it was because quasi-determinism is "...or **error**". I think we actually do need it here.

Lemma 2.3 (Clash). *If $\langle S;\, e\rangle \hookrightarrow \langle S';\, e'\rangle$ (where $\langle S';\, e'\rangle \neq$ **error**), then for all S'' such that S'' is non-conflicting with $\langle S;\, e\rangle \hookrightarrow \langle S';\, e'\rangle$ and $S' \sqcup_S S'' = \top_S$:*

$\langle S \sqcup_S S'';\, e\rangle \hookrightarrow^{i}$ **error**, *where $i \leq 1$.*

Proof. By induction on the derivation of $\langle S;\ e\rangle \hookrightarrow \langle S';\ e'\rangle$, by cases on the last rule in the derivation; see Section A.3. □

2.5.4. Error Preservation lemma.

Lemma 2.4, Error Preservation, says that if a configuration $\langle S;\ e\rangle$ steps to **error**, then evaluating e in the context of some larger store will also result in **error**.

LK: We didn't need the Error Preservation lemma for the quasi-determinism proof, but I'm pretty sure the only reason we didn't need it was because quasi-determinism is "...or **error**". I think we actually do need it here.

Lemma 2.4 (Error Preservation). *If* $\langle S;\ e\rangle \hookrightarrow$ **error** *and* $S \sqsubseteq_S S'$*, then* $\langle S';\ e\rangle \hookrightarrow$ **error**.

TODO: Figure out if we even actually need this property, and if so, what to do here. If we do need it, then do we only need to handle E-Eval-Ctxt and E-Put-Err, or do we need to look at all the cases?

2.5.5. Confluence lemmas.

Lemma 2.5, the Strong Local Confluence lemma, says that if a configuration σ can step to configurations σ_a and σ_b, then there exists an configuration σ_c that σ_a and σ_b can each reach in at most one step. Lemmas 2.6 and 2.7 then generalize that result to arbitrary numbers of steps.

The structure of this part of the proof differs slightly from the Budimlić *et al.* determinism proof for Featherweight CnC. Budimlić *et al.* prove a *diamond* property, in which σ_a and σ_b each step to σ_c in *exactly* one step. They then get a property like Lemma 2.5 as an immediate consequence of the diamond property, by choosing $i = j = 1$. But a true diamond property with exactly one step "on each side of the diamond" is stronger than we need here, and, in fact, does not hold for λ_{LVar}; so, instead, I prove the weaker "at most one step" property directly as Lemma 2.5.

Lemma 2.5 (Strong Local Confluence). *If* $\sigma \hookrightarrow \sigma_a$ *and* $\sigma \hookrightarrow \sigma_b$*, then there exist* σ_c, i, j *such that* $\sigma_a \hookrightarrow^i \sigma_c$ *and* $\sigma_b \hookrightarrow^j \sigma_c$ *and* $i \leq 1$ *and* $j \leq 1$*. TODO: Figure out if we need to mention permutations in the statement of the proof.*

Proof. By induction on the derivation of $\sigma \hookrightarrow \sigma_a$, by cases on the last rule in the derivation; see Section A.5. □

Lemma 2.6 (Strong One-Sided Confluence). *If $\sigma \hookrightarrow \sigma'$ and $\sigma \hookrightarrow^m \sigma''$, where $1 \leq m$, then there exist σ_c, i, j such that $\sigma' \hookrightarrow^i \sigma_c$ and $\sigma'' \hookrightarrow^j \sigma_c$ and $i \leq m$ and $j \leq 1$. TODO: If the statement of Lemma 2.5 changes to mention permutations, then figure out how the statement of this one has to change as well.*

Proof. By induction on m; see Section A.6. □

Lemma 2.7 (Strong Confluence). *If $\sigma \hookrightarrow^n \sigma'$ and $\sigma \hookrightarrow^m \sigma''$, where $1 \leq n$ and $1 \leq m$, then there exist σ_c, i, j such that $\sigma' \hookrightarrow^i \sigma_c$ and $\sigma'' \hookrightarrow^j \sigma_c$ and $i \leq m$ and $j \leq n$. TODO: If the statement of Lemma 2.5 changes to mention permutations, then figure out how the statement of this one has to change as well.*

Proof. By induction on n; see Section A.7. □

Lemma 2.8 (Confluence). *If $\sigma \hookrightarrow^* \sigma'$ and $\sigma \hookrightarrow^* \sigma''$, then there exists σ_c such that $\sigma' \hookrightarrow^* \sigma_c$ and $\sigma'' \hookrightarrow^* \sigma_c$. TODO: If the statement of Lemma 2.5 changes to mention permutations, then figure out how the statement of this one has to change as well.*

Proof. Strong Confluence (Lemma 2.7) implies Confluence. □

2.5.6. Determinism theorem. Finally, the determinism theorem, Theorem 2.1, is a direct result of Lemma 2.8:

Theorem 2.1 (Determinism). *If $\sigma \hookrightarrow^* \sigma'$ and $\sigma \hookrightarrow^* \sigma''$, and neither σ' nor σ'' can take a step, then $\sigma' = \sigma''$. TODO: If the statement of Lemma 2.5 changes to mention permutations, then figure out how the statement (and proof) of this one has to change as well.*

Proof. We have from Lemma 2.8 that there exists σ_c such that $\sigma' \hookrightarrow^* \sigma_c$ and $\sigma'' \hookrightarrow^* \sigma_c$. Since neither σ' nor σ'' can take a step, we must have $\sigma' = \sigma_c$ and $\sigma'' = \sigma_c$, hence $\sigma' = \sigma''$. □

2.5.7. Discussion: termination. I have followed Budimlić *et al.* [**9**] in treating *determinism* separately from the issue of *termination*. Yet one might legitimately be concerned that in λ_{LVar}, a configuration could have both an infinite reduction path and one that terminates with a value. Theorem 2.1 says that if two runs of a given λ_{LVar} program reach configurations where no more reductions are possible, then they have reached the same configuration. Hence Theorem 2.1 handles the case of *deadlocks* already: a λ_{LVar} program can deadlock (*e.g.*, with a blocked `get`), but it will do so deterministically.

However, Theorem 2.1 has nothing to say about *livelocks*, in which a program reduces infinitely. It would be desirable to have a *consistent termination* property which would guarantee that if one run of a given λ_{LVar} program terminates with a non-**error** result, then every run will. I conjecture (but do not prove) that such a consistent termination property holds for λ_{LVar}. Such a property could be paired with Theorem 2.1 to guarantee that if one run of a given λ_{LVar} program terminates in a non-**error** configuration σ, then every run of that program terminates in σ. (The "non-**error** configuration" condition is necessary because it is possible to construct a λ_{LVar} program that can terminate in **error** on some runs and diverge on others. By contrast, the existing determinism theorem does not have to treat **error** specially.)

2.6. Generalizing the `put` and `get` operations

TODO: Write this section!

2.6.1. Generalizing from least-upper-bound writes to inflationary, commutative writes.

TODO: Write this subsection!

LK: This will be about generalized inflationary+commutative writes, rather than least-upper-bound writes (lub is a special case of this).

TODO: Say something about how the lattice in Figure 2.2(c) has different semantics if we have least-upper-bound writes or incremental writes, and how incremental writes may in fact be what is desired. Possibly cite the CRDTs work and forward-reference Chapter 5.

LK: Here I can probably reuse some material from the PLDI and DISC papers and from my thesis proposal.

2.6.2. A more general formulation of threshold sets.

TODO: Write this subsection!

LK: This will be about generalized threshold sets, rather than simple threshold sets (i.e., from our DISC '14 submission); explain how the threshold sets that we've seen so far are a special case of this).

2.6.3. Generalizing from threshold sets to threshold functions.

TODO: Write this subsection!

LK: This will be about ”threshold functions”, rather than either simple threshold sets or generalized threshold sets (i.e., partial functions that take a lattice element and are undefined for all inputs that are not at or above a given point in the lattice, and constant for all inputs that are at or above that point; both kinds of threshold sets are a special case of this, afaict).

CHAPTER 3

Quasi-deterministic and event-driven programming with LVars

The LVars programming model presented in Chapter 2 is based on the idea of *monotonic data structures*, in which (1) information can only be added, never removed, and (2) the order in which information is added is not observable. A paradigmatic example is a set that supports insertion but not removal, but there are many others. In the LVars model, all shared data structures (called LVars) are monotonic, and the states that an LVar can take on form a *lattice*. Writes to an LVar must correspond to a least upper bound operation in the lattice, which means that they monotonically increase the information in the LVar, and that they commute with one another. But commuting writes are not enough to guarantee determinism: if a read can observe whether or not a concurrent write has happened, then it can observe differences in scheduling. So, in the LVars model, the answer to the question "has a write occurred?" (*i.e.*, is the LVar above a certain lattice value?) is always *yes*; the reading thread will block until the LVar's contents reach a desired threshold. In a monotonic data structure, the absence of information is transient—another thread could add that information at any time—but the presence of information is forever.

The LVars model guarantees determinism and supports an unlimited variety of shared data structures: anything viewable as a lattice. However, it is not as general-purpose as one might hope. Consider again the challenge problem for deterministic-by-construction parallel programming that we saw in Chapter 2:

> In a directed graph, find the connected component containing a vertex v, and compute a (possibly expensive) function f over all vertices in that component, making the set of results available asynchronously to other computations.

In Section 2.1, we considered an attempt at a solution for this problem using purely functional parallelism (shown in Figure 2.1). Unfortunately, our purely functional attempt did not quite satisfy the above specification: although connected component discovery proceeded in parallel, members of the output set did not become available to other computations until the entire connected component had been traversed, limiting parallelism.

What would happen if we tried to solve this problem using LVars? A typical implementation of the graph-traversal part of the problem—including the purely functional implementation of Section 2.1—involves a monotonically growing set of "seen nodes"; neighbors of seen nodes are fed back into the set until it reaches a fixed point. Such fixpoint computations are ubiquitous, and would seem to be a perfect match for the LVars model due to their use of monotonicity. But they are not expressible using the threshold read and least-upper-bound write operations of the basic LVars model.

The problem is that these computations rely on *negative* information about a monotonic data structure, *i.e.*, on the *absence* of certain writes to the data structure. In a graph traversal, for example, neighboring nodes should only be explored if the current node is *not yet* in the set; a fixpoint is reached only if no new neighbors are found; and, of course, at the end of the computation it must be possible to learn exactly which nodes were reachable (which entails learning that certain nodes were not). But in the LVars model, asking whether a node is in a set means waiting until the node *is* in the set, and it is not clear how to lift this restriction while retaining determinism.

In this chapter, I describe two extensions to the basic LVars model of Chapter 2 that make it possible for monotonic data structures to "say no":

- First, I extend the model with a primitive operation `freeze` for *freezing* an LVar, which comes with the following tradeoff: once an LVar is frozen, any further writes that would change its value instead throw an exception; on the other hand, it becomes possible to discover the exact value of the LVar, learning both positive and negative information about it, without blocking.
- Second, I add the ability to attach *event handlers* to an LVar. When an event handler has been registered with an LVar, it invokes a *callback function* to run asynchronously, whenever events arrive (in the form of monotonic updates to the LVar). Ordinary LVar reads encourage a synchronous, *pull* model of programming in which threads ask specific questions of an LVar, potentially blocking

> until the answer is "yes". Handlers, by contrast, support an asynchronous, *push* model of programming. Crucially, it is possible to check for *quiescence* of a handler, discovering that no callbacks are currently enabled—a transient, negative property. Since quiescence means that there are no further changes to respond to, it can be used to tell that a fixpoint has been reached.

Unfortunately, freezing does not commute with writes that change an LVar.[1] If a freeze is interleaved before such a write, the write will raise an exception; if it is interleaved afterwards, the program will proceed normally. It would appear that the price of negative information is the loss of determinism!

Fortunately, the loss is not total. Although LVar programs with freezing are not guaranteed to be deterministic, they do satisfy a related property that I call *quasi-determinism*: all executions that produce a final value produce the *same* final value. To put it another way, a quasi-deterministic program can be trusted to never change its answer due to nondeterminism; at worst, it might raise an exception on some runs. This exception can in principle pinpoint the exact pair of freeze and write operations that are racing, greatly easing debugging.

In general, the ability to make exact observations of the contents of data structures is in tension with the goal of guaranteed determinism. Since pushing towards full-featured, general monotonic data structures leads to flirtation with nondeterminism, perhaps the best way of ultimately getting deterministic outcomes is to traipse a short distance into nondeterministic territory, and make our way back. The identification of quasi-deterministic programs as a useful intermediate class of programs is a contribution of this dissertation. That said, in many cases the `freeze` construct is only used as the very final step of a computation: after a global barrier, freezing is used to extract an answer. In this common case, determinism is guaranteed, since no writes can subsequently occur.

I will refer to the LVars model, extended with handlers, quiescence, and freezing, as the *LVish model*. The rest of this chapter is organized as follows: in Section 3.1, I introduce the LVish programming model informally, through a series of examples. I will also return to the graph traversal I discussed above and show how to implement it using the LVish Haskell library (which I will go on to discuss the internals of in Chapter 4).

[1] The same is true for quiescence detection; see Section 3.1.2.

Then, in Section 3.2, I formalize the LVish model by extending the λ_{LVar} calculus of Chapter 2 to add support for handlers, quiescence, and freezing, calling the resulting language λ_{LVish}. The main technical result of this chapter is a proof of quasi-determinism for λ_{LVish} (Section **??**). Just as with the determinism proof I gave for λ_{LVar} in Chapter 2, the quasi-determinism proof for λ_{LVish} relies on an Independence lemma (Section 3.3.2) that captures the commutative effects of LVar computations.

3.1. LVish, informally

While LVars offer a deterministic programming model that allows communication through a wide variety of data structures, they are not powerful enough to express common algorithmic patterns, like fixpoint computations, that require both positive and negative queries. In this section, I explain our extensions to the LVars model at a high level; Section 3.2 then formalizes them.

3.1.1. Asynchrony through event handlers. Our first extension to LVars is the ability to do asynchronous, event-driven programming through event handlers. An *event* for an LVar can be represented by a lattice element; the event *occurs* when the LVar's current value reaches a point at or above that lattice element. An *event handler* ties together an LVar with a callback function that is asynchronously invoked whenever some events of interest occur.

To illustrate how event handlers work, consider again the lattice of Figure 2.2(a) from Chapter 2. Suppose that *lv* is an LVar whose states correspond to this lattice. The expression

(Example 3.1) $$\texttt{addHandler}\ \mathit{lv}\ \{1, 3, 5, \dots\}\ (\lambda x.\, \texttt{put}\ \mathit{lv}\ x+1)$$

registers a handler for *lv* that executes the callback function $\lambda x.\, \texttt{put}\ \mathit{lv}\ x+1$ for each odd number that *lv* is at or above. When Example 3.1 is finished evaluating, *lv* will contain the smallest even number that is at or above what its original value was. For instance, if *lv* originally contains 4, the callback function will be invoked twice, once with 1 as its argument and once with 3. These calls will respectively write $1+1=2$ and $3+1=4$ into *lv*; since both writes are ≤ 4, *lv* will remain 4. On the other hand, if *lv* originally contains 5, then the callback will run three times, with $1, 3$, and 5 as its respective arguments, and with the latter of these calls writing $5+1=6$ into *lv*, leaving *lv* as 6.

In general, the second argument to addHandler, which I call an *event set*, is an arbitrary subset Q of the LVar's lattice, specifying which events should be handled.[2] Event handlers in the LVish model are somewhat unusual in that they invoke their callback for *all* events in their event set Q that have taken place (*i.e.*, all values in Q less than or equal to the current LVar value), even if those events occurred prior to the handler being registered. To see why this semantics is necessary, consider the following, more subtle example (written in a hypothetical language with a semantics similar to that of λ_{LVar}, but with the addition of addHandler):

(Example 3.2)
$$\begin{aligned}
\texttt{let par}\ \_ &= \texttt{put}\ \mathit{lv}\ 0 \\
\_ &= \texttt{put}\ \mathit{lv}\ 1 \\
\_ &= \texttt{addHandler}\ \mathit{lv}\ \{0,1\}\ (\lambda x.\ \texttt{if}\ x = 0\ \texttt{then}\ \texttt{put}\ \mathit{lv}\ 2) \\
\texttt{in}\ \texttt{get}\ \mathit{lv}\ \ \{2\}&
\end{aligned}$$

Can Example 3.2 ever block? If a callback only executed for events that arrived after its handler was registered, or only for the largest event in its event set that had occurred, then the example would be nondeterministic: it would block, or not, depending on how the handler registration was interleaved with the puts. By instead executing a handler's callback once for *each and every* element in its event set below or at the LVar's value, we guarantee quasi-determinism—and, for Example 3.2, guarantee the result of 2.

The power of event handlers is most evident for lattices that model collections, such as sets. For example, if we are working with lattices of sets of natural numbers, ordered by subset inclusion, then we can write the following function:

$$\texttt{forEach} = \lambda \mathit{lv}.\ \lambda f.\ \texttt{addHandler}\ \mathit{lv}\ \{\{0\},\{1\},\{2\},\dots\}\ f$$

Unlike the usual forEach function found in functional programming languages, this function sets up a *permanent*, asynchronous flow of data from *lv* into the callback f. Functions like forEach can be used to set up complex, cyclic data-flow networks, as we will see in Section 4.3.

[2] Like threshold sets, these event sets are a mathematical modeling tool only; they have no explicit existence in the LVish library implementation.

In writing `forEach`, we consider only the singleton sets to be events of interest, which means that if the value of *lv* is some set like $\{2, 3, 5\}$ then f will be executed once for each singleton subset ($\{2\}$, $\{3\}$, $\{5\}$)—that is, once for each element. In Section 4.2.2, we will see that this kind of event set can be specified in a lattice-generic way, and in Section 4.2 we will see that it corresponds closely to our implementation strategy.

3.1.2. Quiescence through handler pools. Because event handlers are asynchronous, we need a separate mechanism to determine when they have reached a *quiescent* state, *i.e.*, when all callbacks for the events that have occurred have finished running. As we saw in the introduction to this chapter, detecting quiescence is crucial for implementing fixpoint computations. To build flexible data-flow networks, it is also helpful to be able to detect quiescence of multiple handlers simultaneously. Thus, our design includes *handler pools*, which are groups of event handlers whose collective quiescence can be tested.

The simplest way to program with handler pools is to use a pattern like the following:

```
let h = newPool
  in addInPool h lv Q f;
     quiesce h
```

where *lv* is an LVar, Q is an event set, and f is a callback. Handler pools are created with the `newPool` function, and handlers are registered with `addHandlerInPool`, a variant of `addHandler` that takes a handler pool as an additional argument. Finally, `quiesce` takes a handler pool as its argument and blocks until all of the handlers in the pool have reached a quiescent state.

Of course, whether or not a handler is quiescent is a non-monotonic property: we can move in and out of quiescence as more `puts` to an LVar occur, and even if all states at or below the current state have been handled, there is no way to know that more `puts` will not arrive to move the LVar's state upwards in the lattice and trigger more callbacks. Early quiescence no risk to quasi-determinism, however, because `quiesce` does not yield any information about *which* events have been handled—any such questions must be asked through LVar functions like `get`. In practice, `quiesce` is almost always used together with freezing, which I explain next.

3.1.3. Freezing and the "freeze-after" pattern. Our final addition to the LVar model is the ability to *freeze* an LVar, which forbids further changes to it, but in return allows its exact value to be read. We expose freezing through the function `freeze`, which takes an LVar as its sole argument, and returns the exact value of the LVar as its result. Any `puts` that would change the value of a frozen LVar instead raise an exception, and it is the potential for races between such `puts` and `freeze` that makes the LVish model quasi-deterministic, rather than fully deterministic.

Putting all the above pieces together, we arrive at a particularly common pattern of programming in the LVish model:

$$
\begin{aligned}
\texttt{freezeAfter} = \lambda \mathit{lv}.\, \lambda Q.\, \lambda f.\ & \texttt{let}\, h \ = \ \texttt{newPool} \\
& \texttt{in}\ \texttt{addInPool}\, h\, \mathit{lv}\, Q\ f; \\
& \quad \texttt{quiesce}\, h; \\
& \quad \texttt{freeze}\, \mathit{lv}
\end{aligned}
$$

In this pattern, an event handler is registered for an LVar, subsequently quiesced, and then the LVar is frozen and its exact value is returned.

3.1.4. A parallel graph traversal using handlers, quiescence, and freezing. We can use the new features in LVish to write a parallel graph traversal in the following simple fashion:

```
traverse :: Graph → NodeLabel → Par (Set NodeLabel)
traverse g startV = do
  seen ← newEmptySet
  putInSet seen startV
  let handle node = parMapM (putInSet seen) (nbrs g node)
  freezeSetAfter seen handle
```

This code, written using the LVish Haskell library (which I will go on to describe in Chapter 4), discovers (in parallel) the set of nodes in a graph g reachable from a given node `startV`, and is guaranteed to produce a deterministic result.[3] It works by creating a fresh `Set` LVar (corresponding to a lattice whose elements are sets, with set union as least upper bound), and seeding it with the starting node.

[3] In the LVish library, the `Par` type constructor is the monad in which LVar computations run; see Chapter 4 for details.

The `freezeSetAfter` function implements a set-specific variant of the freeze-after pattern I described above. It combines freezing and event handlers: first, it registers the callback `handle` as a handler for the `seen` set, which will asynchronously put the neighbors of each visited node into the set, possibly triggering further callbacks, recursively. Second, when no further callbacks are ready to run—*i.e.*, when the `seen` set has reached a fixpoint—`freezeSetAfter` will freeze the set and return its exact value.

3.2. LVish, formally

In this section, I present λ_{LVish}, a core calculus for the LVish programming model. λ_{LVish} is a quasi-deterministic, parallel, call-by-value λ-calculus extended with a store containing LVars. It extends the original λ_{LVar} language of Chapter 2 to support the new features in the LVish model that I described in the previous section. In comparison to the informal description in Section 3.1, though, I make two simplifications to keep the model lightweight:

- As with λ_{LVar} in Chapter 2, I parameterize the definition of λ_{LVish} by a *single* application-specific lattice, representing the set of states that LVars in the calculus can take on. Therefore λ_{LVish} is really a *family* of calculi, varying by choice of lattice. Multiple lattices can in principle be encoded using a sum construction, so this modeling choice is just to keep the presentation simple; in any case, our Haskell implementation supports multiple lattices natively.
- Rather than modeling the full ensemble of event handlers, handler pools, quiescence, and freezing as separate primitives, I instead formalize the "freeze-after" pattern—which combined them—directly as a primitive. This greatly simplifies the calculus, while still capturing the essence of the programming model.

3.2.1. Lattices. Just as with λ_{LVar}, the application-specific lattice is given as a 4-tuple $(D, \sqsubseteq, \bot, \top)$ where D is a set, $\sqsubseteq$ is a partial order on the elements of D, $\bot$ is the least element of D according to $\sqsubseteq$ and $\top$ is the greatest. The $\bot$ element represents the initial "empty" state of every LVar, while $\top$ represents the "error" state that would result from conflicting updates to an LVar. The partial order $\sqsubseteq$ represents the order in which an LVar may take on states. It induces a binary *least upper bound* (lub) operation $\sqcup$ on the elements of D.

Every two elements of D must have a least upper bound in D. Intuitively, the existence of a lub for every two elements of D means that it is possible for two subcomputations to independently update an LVar, and then deterministically merge the results by taking the lub of the resulting two states. Formally, this makes $(D, \sqsubseteq, \bot, \top)$ a *bounded join-semilattice* with a designated greatest element $\top$; I continue to use "lattice" as shorthand, and I use D as a shorthand for the entire 4-tuple $(D, \sqsubseteq, \bot, \top)$ when its meaning is clear from the context.

3.2.2. Freezing. To model freezing, we need to generalize the notion of the state of an LVar to include information about whether it is "frozen" or not. Thus, in λ_{LVish} an LVar's *state* is a pair $(d, \textit{frz})$, where d is an element of the application-specific set D and *frz* is a "status bit" of either true or false. A state where *frz* is false is "unfrozen", and one where *frz* is true is "frozen".

I define an ordering $\sqsubseteq_p$ on LVar states $(d, \textit{frz})$ in terms of the application-specific ordering $\sqsubseteq$ on elements of D. Every element of D is "freezable" except $\top$. Informally:

- Two unfrozen states are ordered according to the application-specific $\sqsubseteq$; that is, $(d, \text{false}) \sqsubseteq_p (d', \text{false})$ exactly when $d \sqsubseteq d'$.
- Two frozen states do not have an order, unless they are equal: $(d, \text{true}) \sqsubseteq_p (d', \text{true})$ exactly when $d = d'$.
- An unfrozen state (d, false) is less than or equal to a frozen state (d', true) exactly when $d \sqsubseteq d'$.
- The only situation in which a frozen state is less than an unfrozen state is if the unfrozen state is $\top$; that is, $(d, \text{true}) \sqsubseteq_p (d', \text{false})$ exactly when $d' = \top$.

Adding status bits to each element (except $\top$) of the lattice $(D, \sqsubseteq, \bot, \top)$ results in a new lattice $(D_p, \sqsubseteq_p, \bot_p, \top_p)$. (The p stands for pair, since elements of this new lattice are pairs $(d, \textit{frz})$.) I write $\sqcup_p$ for the least upper bound operation that $\sqsubseteq_p$ induces. Definitions 3.1 and 3.2 and Lemmas 3.1 and 3.2 formalize this notion.

Definition 3.1. Suppose $(D, \sqsubseteq, \bot, \top)$ is a lattice. We define an operation Freeze$(D, \sqsubseteq, \bot, \top) \overset{\triangle}{=} (D_p, \sqsubseteq_p, \bot_p, \top_p)$ as follows:

(1) D_p is a set defined as follows:

$$\begin{aligned} D_p \triangleq & \{(d, \mathit{frz}) \mid d \in (D - \{\top\}) \wedge \mathit{frz} \in \{\text{true}, \text{false}\}\} \\ & \cup \{(\top, \text{false})\} \end{aligned}$$

(2) $\sqsubseteq_p \in \mathcal{P}(D_p \times D_p)$ is a binary relation defined as follows:

$$\begin{array}{lcccl} (d, \text{false}) & \sqsubseteq_p & (d', \text{false}) & \iff & d \sqsubseteq d' \\ (d, \text{true}) & \sqsubseteq_p & (d', \text{true}) & \iff & d = d' \\ (d, \text{false}) & \sqsubseteq_p & (d', \text{true}) & \iff & d \sqsubseteq d' \\ (d, \text{true}) & \sqsubseteq_p & (d', \text{false}) & \iff & d' = \top \end{array}$$

(3) $\bot_p \triangleq (\bot, \text{false})$.

(4) $\top_p \triangleq (\top, \text{false})$.

Lemma 3.1 (Partition of D_p). *Suppose* $(D, \sqsubseteq, \bot, \top)$ *is a lattice, and that* $(D_p, \sqsubseteq_p, \bot_p, \top_p) = \text{Freeze}(D, \sqsubseteq, \bot, \top)$*, and let* $X = D - \{\top\}$*. Then every member of* D_p *is either*

- (d, false)*, with* $d \in D$*, or*
- (x, true)*, with* $x \in X$.

Proof. Immediate from Definition 3.1. □

Definition 3.2. We define a binary operator $\sqcup_p \in D_p \times D_p \to D_p$ as follows:

$$\begin{array}{lcl} (d_1, \text{false}) \sqcup_p (d_2, \text{false}) & = & (d_1 \sqcup d_2, \text{false}) \\ (d_1, \text{true}) \sqcup_p (d_2, \text{true}) & = & \begin{cases} (d_1, \text{true}) & \text{if } d_1 = d_2 \\ (\top, \text{false}) & \text{otherwise} \end{cases} \\ (d_1, \text{false}) \sqcup_p (d_2, \text{true}) & = & \begin{cases} (d_2, \text{true}) & \text{if } d_1 \sqsubseteq d_2 \\ (\top, \text{false}) & \text{otherwise} \end{cases} \\ (d_1, \text{true}) \sqcup_p (d_2, \text{false}) & = & \begin{cases} (d_1, \text{true}) & \text{if } d_2 \sqsubseteq d_1 \\ (\top, \text{false}) & \text{otherwise} \end{cases} \end{array}$$

Lemma 3.2 says that if $(D, \leq, \bot, \top)$ is a lattice, then $(D_p, \sqsubseteq_p, \bot_p, \top_p)$ is as well:

Lemma 3.2 (Lattice structure). *Suppose that* $(D, \sqsubseteq, \bot, \top)$ *is a lattice, and that* $(D_p, \sqsubseteq_p, \bot_p, \top_p) = \text{Freeze}(D, \sqsubseteq, \bot, \top)$. *Then:*

(1) $\sqsubseteq_p$ *is a partial order over* D_p.

(2) *Every nonempty finite subset of* D_p *has a least upper bound.*

(3) $\bot_p$ *is the least element of* D_p.

(4) $\top_p$ *is the greatest element of* D_p.

Therefore $(D_p, \sqsubseteq_p, \bot_p, \top_p)$ *is a lattice.*

Proof. See Section A.8. □

3.2.3. Stores. During the evaluation of λ_{LVish} programs, a *store* S keeps track of the states of LVars. Each LVar is represented by a binding from a location l, drawn from a set *Loc*, to its state, which is some pair (d, frz) from the set D_p. The way that stores are handled in λ_{LVish} is very similar to how they are handled in λ_{LVar}, except that store bindings now point to states (d, frz), that is, elements of D_p, instead of merely to d, that is, elements of D.

Definition 3.3. A *store* is either a finite partial mapping $S : \mathit{Loc} \overset{\text{fin}}{\rightarrow} (D_p - \{\top_p\})$, or the distinguished element $\top_S$.

I use the notation $S[l \mapsto (d, \mathit{frz})]$ to denote extending S with a binding from l to (d, frz). If $l \in \mathit{dom}(S)$, then $S[l \mapsto (d, \mathit{frz})]$ denotes an update to the existing binding for l, rather than an extension. Another way to denote a store is by explicitly writing out all its bindings, using the notation $[l_1 \mapsto (d_1, \mathit{frz}_1), l_2 \mapsto (d_2, \mathit{frz}_2), \ldots]$.

We can lift the $\sqsubseteq_p$ and $\sqcup_p$ operations defined on elements of D_p to the level of stores:

Definition 3.4. A store S is *less than or equal to* a store S' (written $S \sqsubseteq_S S'$) iff:

- $S' = \top_S$, or
- $\mathit{dom}(S) \subseteq \mathit{dom}(S')$ and for all $l \in \mathit{dom}(S)$, $S(l) \sqsubseteq_p S'(l)$.

Definition 3.5. The *least upper bound (lub)* of two stores S_1 and S_2 (written $S_1 \sqcup_S S_2$) is defined as follows:

- $S_1 \sqcup_S S_2 = \top_S$ iff $S_1 = \top_S$ or $S_2 = \top_S$.
- $S_1 \sqcup_S S_2 = \top_S$ iff there exists some $l \in \mathit{dom}(S_1) \cap \mathit{dom}(S_2)$ such that $S_1(l) \sqcup_p S_2(l) = \top_p$.
- Otherwise, $S_1 \sqcup_S S_2$ is the store S such that:
  - $\mathit{dom}(S) = \mathit{dom}(S_1) \cup \mathit{dom}(S_2)$, and
  - For all $l \in \mathit{dom}(S)$:

$$S(l) = \begin{cases} S_1(l) \sqcup_p S_2(l) & \text{if } l \in \mathit{dom}(S_1) \cap \mathit{dom}(S_2) \\ S_1(l) & \text{if } l \notin \mathit{dom}(S_2) \\ S_2(l) & \text{if } l \notin \mathit{dom}(S_1) \end{cases}$$

If, for example,

$$(d_1, \mathit{frz}_1) \sqcup_p (d_2, \mathit{frz}_2) = \top_p,$$

then

$$[l \mapsto (d_1, \mathit{frz}_1)] \sqcup_S [l \mapsto (d_2, \mathit{frz}_2)] = \top_S.$$

Just as a a store containing a binding $l \mapsto \top$ can never arise during the execution of a λ_{LVar} program, a store containing a binding $l \mapsto (\top, \mathit{frz})$ can never arise during the execution of a λ_{LVish} program. An attempted put that would take the value of l to $(\top, \text{false})$—that is, $\top_p$—will raise an error, and there is no $(\top, \text{true})$ element of D_p.

3.2.4. λ_{LVish}: syntax and semantics.

Given a lattice $(D, \sqsubseteq, \bot, \top)$ with elements $d \in D$:

$$\begin{array}{rlll}
\text{configurations} & \sigma & ::= & \langle S;\, e\rangle \mid \textbf{error} \\
\text{expressions} & e & ::= & x \mid v \mid e\,e \mid \texttt{get}\,e\,e \mid \texttt{put}\,e\,e \mid \texttt{new} \mid \texttt{freeze}\,e \\
 & & \mid & \texttt{freeze}\,e\,\texttt{after}\,e\,\texttt{with}\,e \\
 & & \mid & \texttt{freeze}\,l\,\texttt{after}\,Q\,\texttt{with}\,\lambda x.\,e, \{e, \dots\}, H \\
\text{values} & v & ::= & \texttt{()} \mid d \mid p \mid l \mid P \mid Q \mid \lambda x.\,e \\
\text{threshold sets} & P & ::= & \{p_1,\, p_2,\, \dots\} \\
\text{event sets} & Q & ::= & \{d_1,\, d_2,\, \dots\} \\
\text{“handled” sets} & H & ::= & \{d_1,\, \dots,\, d_n\} \\
\text{stores} & S & ::= & [l_1 \mapsto p_1,\, \dots,\, l_n \mapsto p_n] \mid \top_S \\
\text{states} & p & ::= & (d, \mathit{frz}) \\
\text{status bits} & \mathit{frz} & ::= & \text{true} \mid \text{false} \\
\text{evaluation contexts} & E & ::= & [\,] \mid E\,e \mid e\,E \mid \texttt{get}\,E\,e \mid \texttt{get}\,e\,E \mid \texttt{put}\,E\,e \mid \texttt{put}\,e\,E \\
 & & \mid & \texttt{freeze}\,E \mid \texttt{freeze}\,E\,\texttt{after}\,e\,\texttt{with}\,e \\
 & & \mid & \texttt{freeze}\,e\,\texttt{after}\,E\,\texttt{with}\,e \mid \texttt{freeze}\,e\,\texttt{after}\,e\,\texttt{with}\,E \\
 & & \mid & \texttt{freeze}\,v\,\texttt{after}\,v\,\texttt{with}\,v, \{e \dots\ E\,e \dots\}, H
\end{array}$$

Figure 3.1. Syntax for λ_{LVish}.

Given a lattice $(D, \sqsubseteq, \bot, \top)$ with elements $d \in D$:

$$\mathit{incomp}(P) \overset{\triangle}{=} \forall\, p_1, p_2 \in P.\, (p_1 \neq p_2 \implies p_1 \sqcup_p p_2 = \top_p) \qquad \boxed{\sigma \hookrightarrow \sigma'}$$

E-Eval-Ctxt

$$\frac{\langle S;\, e\rangle \hookrightarrow \langle S';\, e'\rangle}{\langle S;\, E[e]\rangle \hookrightarrow \langle S';\, E[e']\rangle}$$

E-Beta

$$\frac{}{\langle S;\, (\lambda x.\, e)\; v\rangle \hookrightarrow \langle S;\, e[x := v]\rangle}$$

E-New

$$\frac{}{\langle S;\, \texttt{new}\rangle \hookrightarrow \langle S[l \mapsto (\bot, \text{false})];\, l\rangle}\ (l \notin \mathit{dom}(S))$$

E-Put

$$\frac{S(l) = p_1 \qquad p_2 = p_1 \sqcup_p (d_2, \text{false}) \qquad p_2 \neq \top_p}{\langle S;\, \texttt{put}\; l\; d_2\rangle \hookrightarrow \langle S[l \mapsto p_2];\, \texttt{()}\rangle}$$

E-Put-Err

$$\frac{S(l) = p_1 \qquad p_1 \sqcup_p (d_2, \text{false}) = \top_p}{\langle S;\, \texttt{put}\; l\; d_2\rangle \hookrightarrow \textbf{error}}$$

E-Get

$$\frac{S(l) = p_1 \qquad \mathit{incomp}(P) \qquad p_2 \in P \qquad p_2 \sqsubseteq_p p_1}{\langle S;\, \texttt{get}\; l\; P\rangle \hookrightarrow \langle S;\, p_2\rangle}$$

E-Freeze-Init

$$\frac{}{\langle S;\, \texttt{freeze}\; l\; \texttt{after}\; Q\; \texttt{with}\; \lambda x.\, e\rangle \hookrightarrow \langle S;\, \texttt{freeze}\; l\; \texttt{after}\; Q\; \texttt{with}\; \lambda x.\, e, \{\}, \{\}\rangle}$$

E-Spawn-Handler

$$\frac{S(l) = (d_1, \mathit{frz}_1) \qquad d_2 \sqsubseteq d_1 \qquad d_2 \notin H \qquad d_2 \in Q}{\langle S;\, \texttt{freeze}\; l\; \texttt{after}\; Q\; \texttt{with}\; \lambda x.\, e_0, \{e, \dots\}, H\rangle \hookrightarrow \langle S;\, \texttt{freeze}\; l\; \texttt{after}\; Q\; \texttt{with}\; \lambda x.\, e_0, \{e_0[x := d_2], e, \dots\}, \{d_2\} \cup H\rangle}$$

E-Freeze-Final

$$\frac{S(l) = (d_1, \mathit{frz}_1) \qquad \forall d_2\, .\, (d_2 \sqsubseteq d_1 \land d_2 \in Q \Rightarrow d_2 \in H)}{\langle S;\, \texttt{freeze}\; l\; \texttt{after}\; Q\; \texttt{with}\; v, \{v \dots\}, H\rangle \hookrightarrow \langle S[l \mapsto (d_1, \text{true})];\, d_1\rangle}$$

E-Freeze-Simple

$$\frac{S(l) = (d_1, \mathit{frz}_1)}{\langle S;\, \texttt{freeze}\; l\rangle \hookrightarrow \langle S[l \mapsto (d_1, \text{true})];\, d_1\rangle}$$

Figure 3.2. An operational semantics for λ_{LVish}.

The syntax and operational semantics of λ_{LVish} appear in Figures 3.1 and 3.2, respectively. As with λ_{LVar}, both the syntax and semantics are parameterized by the lattice $(D, \sqsubseteq, \bot, \top)$, and the reduction relation $\hookrightarrow$ is defined on *configurations* $\langle S;\ e \rangle$, made up of a store S and an expression e. The *error configuration*, written **error**, is a unique element added to the set of configurations, but $\langle \top_S;\ e \rangle$ is equal to **error** for all expressions e. The metavariable σ ranges over configurations.

λ_{LVish} has all the expression forms of λ_{LVar}—variables, values, application expressions, `get` expressions, `put` expressions, and `new`—and adds two new forms: the `freeze` expression and the $\texttt{freeze} - \texttt{after} - \texttt{with}$ expression, which I discuss in more detail below. Values in λ_{LVish} include all those from λ_{LVar}—the unit value `()`, lattice elements d, locations l, threshold sets P, and λ expressions—as well as states p, which are pairs (d, frz), and event sets Q. Instead of T, I now use the metavariable P for threshold sets, in keeping with the fact that in λ_{LVish}, members of threshold sets are states p.

As with λ_{LVar}, λ_{LVish} uses a reduction semantics based on evaluation contexts. The E-Eval-Ctxt rule allows us to apply reductions within a context, and is identical to the corresponding rule in λ_{LVar}, although the set of evaluation contexts that the metavariable E ranges over has grown to accommodate `freeze` and $\texttt{freeze} - \texttt{after} - \texttt{with}$. The E-Beta rule is also identical to its counterpart in λ_{LVar}.

3.2.5. Semantics of `new`, `put`, and `get`.

Because of the addition of status bits, the E-New, E-Put, E-Put-Err, E-Get rules have changed slightly from their counterparts in λ_{LVar}:

- `new` (implemented by the E-New rule) extends the store with a binding for a new LVar whose initial state is $(\bot, \text{false})$, and returns the location l of that LVar (*i.e.*, a pointer to the LVar).
- `put` (implemented by the E-Put and E-Put-Err rules) takes a pointer to an LVar and a new lattice element d_2 and updates the LVar's state to the *least upper bound* of the current state and (d_2, false), potentially pushing the state of the LVar upward in the lattice. Any update that would take the state of an LVar to $\top_p$ results in the program immediately stepping to **error**.
- `get` (implemented by the E-Get rule) performs a blocking threshold read. It takes a pointer to an LVar and a *threshold set* P, which is a non-empty set of LVar states that must be *pairwise incompatible*, expressed by the premise *incomp*(P). A threshold set P is pairwise incompatible iff the lub of any two distinct elements in P is $\top_p$. If the LVar's state p_1 in the lattice is *at or above* some $p_2 \in P$,

the get operation unblocks and returns p_2. Note that p_2 is a unique element of P, for if there is another $p_2' \neq p_2$ in the threshold set such that $p_2' \sqsubseteq_p p_1$, it would follow that $p_2 \sqcup_p p_2' = p_1 \neq \top_p$, which contradicts the requirement that P be pairwise incompatible.[4]

Is the get operation deterministic? Consider two lattice elements p_1 and p_2 that have no ordering and have $\top_p$ as their lub, and suppose that puts of p_1 and p_2 and a get with $\{p_1, p_2\}$ as its threshold set all race for access to an LVar lv. Eventually, the program is guaranteed to fault, raising **error** by way of the E-Put-Err rule, because $p_1 \sqcup_p p_2 = \top_p$. Before that happens, though, get lv $\{p_1, p_2\}$ could return either p_1 or p_2. Therefore, get *can* behave nondeterministically—but this behavior is not observable in the final outcome of the program.

3.2.6. Freezing and the $\texttt{freeze} - \texttt{after} - \texttt{with}$ primitive. The E-Freeze-Init, E-Spawn-Handler, E-Freeze-Final, and E-Freeze-Simple rules are all new additions to λ_{LVish}. The E-Freeze-Simple rule gives the semantics for the freeze expression, which takes an LVar as argument and immediately freezes and returns its contents.

More interesting is the $\texttt{freeze} - \texttt{after} - \texttt{with}$ primitive, which models the "freeze-after" pattern I described in Section 3.1.3. The expression

$$\texttt{freeze}\ e_{\text{lv}}\ \texttt{after}\ e_{\text{events}}\ \texttt{with}\ e_{\text{cb}}$$

has the following semantics:

- It attaches the callback e_{cb} to the LVar e_{lv}. The expression e_{events} must evaluate to a event set Q; the callback will be executed, once, for each lattice element in Q that the LVar's state reaches or surpasses. The callback e_{cb} is a function that takes a lattice element as its argument. Its return value is ignored, so it runs solely for effect. For instance, a callback might itself do a put to the LVar to which it is attached, triggering yet more callbacks.
- If the handler reaches a quiescent state, the LVar e_{lv} is frozen, and its *exact* state is returned (rather than an underapproximation of the state, as with get).

[4] Although *incomp*(P) is given as a premise of the E-Get reduction rule (suggesting that it is checked at runtime), in a real implementation threshold sets need not be written explicitly, and it is the data structure author's responsibility to ensure that any provided read operations have threshold semantics; see Chapter 4.TODO: Point to a more specific part of Chapter 4.

To keep track of the running callbacks, λ_{LVish} includes an auxiliary form,

$$\texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e, \dots\}\,, H$$

where:

- The value l is the LVar being handled/frozen;
- The set Q (a subset of the lattice D) is the event set;
- The value $\lambda x.\, e_0$ is the callback function;
- The set of expressions $\{e, \dots\}$ are the running callbacks; and
- The set H (a subset of the lattice D) represents those values in Q for which callbacks have already been launched.

Due to λ_{LVish}'s use of evaluation contexts, any running callback can execute at any time, as if each is running in its own thread.

The rule E-Spawn-Handler launches a new callback thread any time the LVar's current value is at or above some element in Q that has not already been handled. This step can be taken nondeterministically at any time after the relevant put has been performed.

The rule E-Freeze-Final detects quiescence by checking that two properties hold. First, every event of interest (lattice element in Q) that has occurred (is bounded by the current LVar state) must be handled (be in H). Second, all existing callback threads must have terminated with a value. In other words, every enabled callback has completed. When such a quiescent state is detected, E-Freeze-Final freezes the LVar's state. Like E-Spawn-Handler, the rule can fire at any time, nondeterministically, that the handler appears quiescent—a transient property! But after being frozen, any further puts that would have enabled additional callbacks will instead fault, causing the program to step to **error**.

Therefore, freezing is a way of "betting" that once a collection of callbacks have completed, no further puts that change the LVar's value will occur. For a given run of a program, either all puts to an LVar arrive before it has been frozen, in which case the value returned by $\texttt{freeze} - \texttt{after} - \texttt{with}$ is the lub of those values, or some put arrives after the LVar has been frozen, in which case the program will fault. And thus we have arrived at *quasi-determinism*: a program will always either evaluate to the same answer or it will fault.

To ensure that we will win our bet, we need to guarantee that quiescence is a *permanent* state, rather than a transient one—that is, we need to perform all `puts` either prior to `freeze − after − with`, or by the callback function within it (as will be the case for fixpoint computations). In practice, freezing is usually the very last step of an algorithm, permitting its result to be extracted. As we will see in Chapter 4, our implementation provides a special `runParThenFreeze` function that does so, and thereby guarantees full determinism.TODO: Point to a more specific part of Chapter 4.

3.3. Proof of quasi-determinism for λ_{LVish}

In this section, I give a proof of quasi-determinism for λ_{LVish} that formalizes the claim made earlier in this chapter: that, for a given program, although some executions may raise exceptions, all executions that produce a final result will produce the same final result.

The quasi-determinism theorem says that if two executions starting from a configuration σ terminate in configurations σ' and σ'', then either σ' and σ'' are the same configuration, or one of them is **error**. As with the determinism result for λ_{LVar}, quasi-determinism follows from a series of supporting lemmas which I first prove. Unlike with the determinism proof for λ_{LVar}, though, for λ_{LVish} I do not need to prove a Clash lemma (*e.g.*, Lemma 2.3) or an Error Preservation lemma (*e.g.*, Lemma 2.4). These properties aren't necessary because quasi-determinism, with its "...or one of them is **error**", is a weaker property than determinism.

3.3.1. Monotonicity lemma. The Monotonicity lemma says that, as evaluation proceeds according to the $\hookrightarrow$ relation, the store can only grow with respect to the $\sqsubseteq_S$ ordering.

Lemma 3.3 (Monotonicity). *If* $\langle S;\, e\rangle \hookrightarrow \langle S';\, e'\rangle$, *then* $S \sqsubseteq_S S'$.

Proof. By induction on the derivation of $\langle S;\, e\rangle \hookrightarrow \langle S';\, e'\rangle$, by cases on the last rule in the derivation; see Section A.9. □

3.3.2. Independence lemma. Like the Independence lemma for λ_{LVar} (Lemma 2.2), Lemma 3.4 establishes a "frame property" for λ_{LVish} that captures the idea that independent effects commute with each other. Just as with the λ_{LVar} version of the Independence lemma, Lemma 3.4 requires as a precondidion that the store S'' must be *non-conflicting* (Definition 2.6) with the original transition from $\langle S;\ e\rangle$ to $\langle S';\ e'\rangle$, meaning that locations in S'' cannot share names with locations newly allocated during the transition, which rules out location name conflicts caused by allocation.

In the context of λ_{LVish}, where freezing is possible, we have an additional precondition that the stores $S' \sqcup_S S''$ and S are *equal in status*—that, for all the locations shared between them, the status bits of those locations agree. This assumption rules out interference from freezing.

Definition 3.6. Two stores S and S' are *equal in status* (written $S =_{\mathit{frz}} S'$) iff for all $l \in (\mathit{dom}(S) \cap \mathit{dom}(S'))$,
if $S(l) = (d, \mathit{frz})$ and $S'(l) = (d', \mathit{frz}')$, then $\mathit{frz} = \mathit{frz}'$.

Lemma 3.4 (Independence). *If $\langle S;\ e\rangle \hookrightarrow \langle S';\ e'\rangle$ (where $\langle S';\ e'\rangle \neq$ **error**), then we have that:*

$\langle S \sqcup_S S'';\ e\rangle \hookrightarrow \langle S' \sqcup_S S'';\ e'\rangle$,

where S'' is any store meeting the following conditions:

- *S'' is non-conflicting with $\langle S;\ e\rangle \hookrightarrow \langle S';\ e'\rangle$,*
- *$S' \sqcup_S S'' =_{\mathit{frz}} S$, and*
- *$S' \sqcup_S S'' \neq \top_S$.*

Proof. By induction on the derivation of $\langle S;\ e\rangle \hookrightarrow \langle S';\ e'\rangle$, by cases on the last rule in the derivation; see Section A.10. □

3.3.3. Quasi-confluence lemmas.

TODO: Add some explanatory text here.

LK: In the POPL paper and TR, there was a lemma called "Strong Local Quasi-Diamond", and another, almost identical one called "Strong Local Quasi-Confluence" that followed almost directly from Strong Local Quasi-Diamond. Here I combine them into a single lemma and call it Strong Local Quasi-Confluence. I don't want to use the word "diamond", since to a lot of people that connotes "exactly one step on each side of the diamond", which isn't true for this language (that is, sometimes it's zero steps). The only reason we were using the word "diamond" was because it was an artifact of the determinism proof in the original FHPC paper, which in turn was an artifact of the CnC paper—see Section 2.5.5 for more commentary on that.

Lemma 3.5 (Strong Local Quasi-Confluence). *TODO: Figure out if we need to mention permutations in the statement of the proof. If $\sigma \hookrightarrow \sigma_a$ and $\sigma \hookrightarrow \sigma_b$, then either:*

(1) *there exist i, j ,and σ_c such that $\sigma_a \hookrightarrow^i \sigma_c$ and $\sigma_b \hookrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$, or*

(2) *$\sigma_a \hookrightarrow$ **error** or $\sigma_b \hookrightarrow$ **error**.*

Proof. By induction on the derivation of $\sigma \hookrightarrow \sigma_a$, by cases on the last rule in the derivation; see Section A.11. □

Lemma 3.6 (Strong One-Sided Quasi-Confluence). *TODO: If the statement of Lemma 3.5 changes to mention permutations, then figure out how the statement of this one has to change as well. If $\sigma \hookrightarrow \sigma'$ and $\sigma \hookrightarrow^m \sigma''$, where $1 \leq m$, then either:*

(1) *there exist σ_c, i, j such that $\sigma' \hookrightarrow^i \sigma_c$ and $\sigma'' \hookrightarrow^j \sigma_c$ and $i \leq m$ and $j \leq 1$, or*

(2) *there exists $k \leq m$ such that $\sigma' \hookrightarrow^k$ **error**, or there exists $k \leq 1$ such that $\sigma'' \hookrightarrow^k$ **error**.*

Proof. By induction on m; see Section A.12. □

Lemma 3.7 (Strong Quasi-Confluence). *TODO: If the statement of Lemma 3.5 changes to mention permutations, then figure out how the statement of this one has to change as well. If $\sigma \hookrightarrow^n \sigma'$ and $\sigma \hookrightarrow^m \sigma''$, where $1 \leq n$ and $1 \leq m$, then either:*

(1) *there exist σ_c, i, j such that $\sigma' \hookrightarrow^i \sigma_c$ and $\sigma'' \hookrightarrow^j \sigma_c$ and $i \leq m$ and $j \leq n$, or*

(2) *there exists $k \leq m$ such that $\sigma' \hookrightarrow^k$ **error**, or there exists $k \leq n$ such that $\sigma'' \hookrightarrow^k$ **error**.*

TODO: Figure out if we need to mention permutations in the statement of the proof.

Proof. By induction on n; see Section A.13. □

Lemma 3.8 (Quasi-Confluence). *TODO: If the statement of Lemma 3.5 changes to mention permutations, then figure out how the statement of this one has to change as well. If $\sigma \hookrightarrow^* \sigma'$ and $\sigma \hookrightarrow^* \sigma''$, then either:*

(1) *there exists σ_c such that $\sigma' \hookrightarrow^* \sigma_c$ and $\sigma'' \hookrightarrow^* \sigma_c$, or*

(2) *$\sigma' =$ **error** or $\sigma'' =$ **error**.*

Proof. Strong Quasi-Confluence (Lemma 3.7) implies Quasi-Confluence. □

3.3.4. Quasi-determinism theorem. The Quasi-Determinism theorem, Theorem 3.1, is a straightforward result of Lemma 3.8. It says that if two executions starting from a configuration σ terminate in configurations σ' and σ'', then σ' and σ'' are the same configuration, or one of them is **error**.

Theorem 3.1 (Quasi-Determinism). *TODO: If the statement of Lemma 3.5 changes to mention permutations, then figure out how the statement (and proof) of this one has to change as well. If $\sigma \hookrightarrow^* \sigma'$ and $\sigma \hookrightarrow^* \sigma''$, and neither σ' nor σ'' can take a step, then either:*

(1) *$\sigma' = \sigma''$, or*

(2) *$\sigma' =$ **error** or $\sigma'' =$ **error**.*

Proof. By Lemma 3.8, one of the following two cases applies:

(1) There exists σ_c such that $\sigma' \hookrightarrow^* \sigma_c$ and $\sigma'' \hookrightarrow^* \sigma_c$. In this case, since neither σ' nor σ'' can step further, we must have $\sigma' = \sigma_c$ and $\sigma'' = \sigma_c$, hence $\sigma' = \sigma''$.

(2) $\sigma' =$ **error** or $\sigma'' =$ **error**, and so the result is immediate.

□

3.3.5. Discussion: quasi-determinism in practice. LK: I kinda threw this subsection in here on a whim. Maybe it should actually go somewhere in Chapter 4, or maybe it should be its own section.

The quasi-determinism result for λ_{LVish} shows that it is not possible to get multiple "answers" from the same program: every run will either produce the same answer or an error. Importantly, this property is true not only for programs that use the freeze-after pattern expressed by the $\texttt{freeze} - \texttt{after} - \texttt{with}$ primitive, but even those that freeze in arbitrary places using the simpler `freeze` primitive. This means that in practice, in a programming model based on LVars with freezing and handlers, even a program that fails to ensure quiescence (introducing the possiblility of a race between a `put` and a `freeze`) cannot produce multiple non-**error** answers.

Therefore the LVish programming model is fundamentally different from one in which the programmer must manually insert synchronization barriers to prevent data races. In that kind of a model, a program with a misplaced synchronization barrier can be fully nondeterministic, producing multiple observable answers. In the LVish model, the worst that can happen is that the program raises an error. Moreover, in the LVish model, an **error** result *always* means that there is an undersynchronization bug in the program, and in principle the error message can even specify exactly which write operation happened after which freeze operation, making it easier to debug the problem.

However, if we *can* ensure that an LVar is only ever frozen *after* all writes to that LVar have completed, then we can guarantee full determinism, because we will have ruled out races between write operations and freeze operations. In the next chapter, I discuss how the LVish Haskell library enforces this "freeze after writing" property.

CHAPTER 4

The LVish Library: Implementation and Evaluation

TODO: Revise this chapter.

LK: What follows is from the FHPC paper and needs to be edited or removed.

4.1. Prototype Implementation and Evaluation

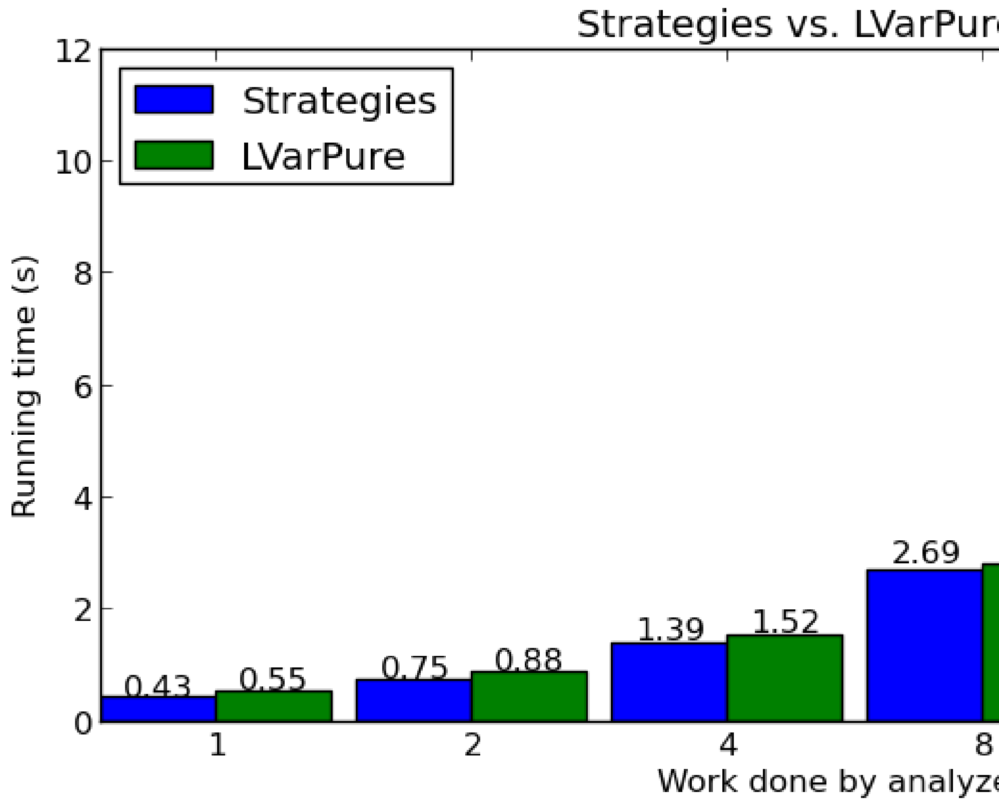
We have implemented a prototype LVars library based on the *monad-par* Haskell library, which provides the `Par` monad [**30**]. Our library, together with example programs and preliminary benchmarking results, is available in in the LVars repository. The relationship to λ_{LVar} is somewhat loose: for instance, while evaluation in λ_{LVar} is always strict, our library allows lazy, pure Haskell computations along with strict, parallel monadic computations.

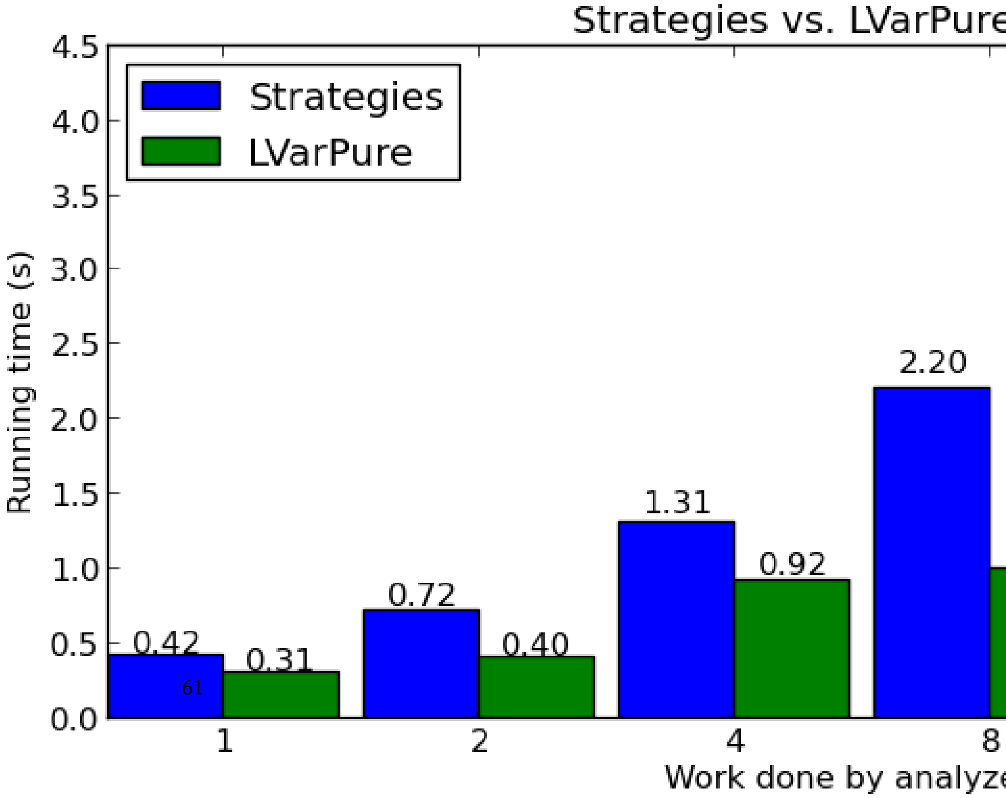
A layered implementation. Use of our LVars library typically involves two parties: first, the data structure author who uses the library directly and provides an implementation of a specific monotonic data structure (*e.g.*, a monotonically growing hashmap), and, second, the application writer who uses that data structure. Only the application writer receives a determinism guarantee; it is the data structure author's obligation to ensure that the states of their data structure form a lattice and that it is only accessible via the equivalent of `put` and `get`.

The data structure author uses an interface provided by our LVars library, which provides core runtime functionality: thread scheduling and tracking of threads blocked on `get` operations. Concretely, the data structure author imports our library and reexports a limited interface specific to their data structure (*e.g.*, for sets, `putInSet` and `waitSetSizeThreshold`). In fact, our library provides three different runtime interfaces for the data structure author to choose among. These "layered" interfaces provide the data structure author with a shifting trade-off between the *ease* of meeting their proof obligation, and *attainable performance*:

```
-- l_acc is an LVar "output parameter":
bf_traverse :: ISet NodeLabel → Graph →
               NodeLabel → Par ()
bf_traverse l_acc g startV =
  do putInSet l_acc startV
     loop {} {startV}
 where loop seen nu =
         if nu == {}
         then return ()
         else do
           let seen' = union seen nu
           allNbr  ← parMap (nbrs g) nu
           allNbr' ← parFold union allNbr
           let nu' = difference allNbr' seen'
           -- Add to the accumulator:
           parMapM (putInSet l_acc) nu'
           loop seen' nu'
-- The function `analyze' is applied to everything
-- that is added to the set `analyzeSet':
go = do analyzedSet ← newSetWith analyze
        res ← bf_traverse analyzedSet profiles profile0
```

Figure 4.1. An example Haskell program, written using our LVars library, that maps a computation over a connected component using a monotonically growing set variable. The code is written in a strict style, using the Par monad for parallelism. The use of the set variable enables modularity and safe pipelining. Consumers can safely asynchronously execute work items put into analyzedSet.


Strategies vs. LVarPur
Strategies
LVarPure
Running time (s)
12
10
8
6
4
2
0
0.43
0.55
0.75
0.88
1.39
1.52
2.69
1
2
4
8
Work done by analyze


Strategies vs. LVarPure
Strategies
LVarPure
Running time (s)
4.5
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
0.42
0.31
0.72
0.40
1.31
0.92
2.20
1
2
4
8
Work done by analyze

(1) **Pure LVars**: Here, each LVar is a single mutable container (an IORef) containing a pure value. This requires only that a library writer select a purely functional data structure and provide a join[1] function for it and a threshold predicate for each get operation. These pure functions are easiest to validate, for example, using the popular QuickCheck [**?**] tool.

(2) **IO LVars**: Pure data structures in mutable containers cannot always provide the best performance for concurrent data structures. Thus we provide a more effectful interface. With it, data structures are represented in terms of arbitrary mutable state; performing a put requires an *update action* (IO) and a get requires an effectful polling function that will be run after any put to the LVar, to determine if the get can unblock.

(3) **Scalable LVars**: Polling each blocked get upon *any* put is not very precise. If the data structure author takes on yet more responsibility, they can use our third interface to reduce contention by managing the storage of blocked computations and threshold functions *themselves*. For example, a concurrent set might store a waitlist of blocked continuations on a per-element basis, rather than using one waitlist for the entire LVar, as in layers (1) and (2).

The support provided to the data structure author *declines* with each of these layers, with the final option providing only parallel scheduling, and little help with defining the specific LVar data structure. But this progressive cost/benefit tradeoff can be beneficial for prototyping and then refining data structure implementations.

Revisiting our breadth-first traversal example. In Section **??**, we proposed using LVars to implement a program that performs a breadth-first traversal of a connected component of a graph, mapping a function over each node in the component. Figure 4.1 gives a version of this program implemented using our LVars library. It performs a breadth-first traversal of the profiles graph with effectful put operations on a shared set variable. This variable, analyzedSet, has to be modified multiple times by putInSet and thus cannot be an IVar.[2] The callback function analyze is “baked into” analyzedSet and may run as soon as new elements are inserted. Our implementation uses the “Pure LVars” runtime layer

[1] Type class Algebra.Lattice.JoinSemiLattice.

[2] Indeed, there are subtle problems with encoding a set even as a linked structure of IVars. For example, if it is represented as a tree, who writes the root?

described above: `analyzedSet` is nothing more than a tree-based data structure (`Data.Set`) stored in a mutable location.

Preliminary benchmarking results. We compared the performance of the LVar-based implementation of `bf_traverse` against the version in Figure 2.1, which we ran using the `Control.Parallel.Strategies` library [**29**], version 3.2.0.3. (Despite being a simple algorithm, even breadth-first search by itself is considered a useful benchmark; in fact, the well-known "Graph 500" [**?**] benchmark is exactly breadth-first search.)

We evaluated the Strategies and LVar versions of `bf_traverse` by running both on a local random directed graph of 40,000 nodes and 320,000 edges (and therefore an average degree of 8), simulating the `analyze` function by doing a specified amount of work for each node, which we varied from 1 to 32 microseconds. Figure 4.2 shows the results of our evaluation on 1, 2, 3, and 4 cores. Although both the Strategies and LVar versions enjoyed a speedup as we added parallel resources, the LVar version scaled particularly well. A subtler, but interesting point is that, in the Strategies version, it took an average of 64.64 milliseconds for the first invocation of `analyze` to begin running after the program began, whereas in the LVar version, it took an average of only 0.18 milliseconds, indicating that the LVar version allows work to be pipelined.

RRN: Report time-to-first-f results in prose I suppose....

LK: What follows is from the POPL paper and needs to be edited.

Our library comes with a number of monotonic data structures, including sets, maps, counters, and single-assignment variables. Further, it can be extended with new data structures, all of which can be used compositionally within the same program. Adding a new data structure typically involves porting an existing scalable (*e.g.*, *lock-free*) data structure to Haskell, then wrapping it to expose a (quasi-)deterministic LVar interface. Our library exposes a monad that is *indexed* by a determinism level: fully deterministic or quasi-deterministic. Thus, the *static type* of an LVish computation reflects its guarantee, and in particular the freeze-last idiom allows freezing

In Section 4.3, we evaluate our library with a case study: parallelizing control flow analysis. The case study begins with an existing implementation of k-CFA [**32**] written in a purely functional style. We show how this code can easily and safely be parallelized by adapting it to the LVish model—an adaptation that yields promising parallel speedup, and also turns out to have benefits even in the sequential case.

4.2. Implementation

We have constructed a prototype implementation of LVish as a monadic library in Haskell, which is available at

`http://hackage.haskell.org/package/lvish`

AJT: Or would we rather link to github?Our library adopts the basic approach of the `Par` monad [**30**], enabling us to employ our own notion of lightweight, library-level threads with a custom scheduler. It supports the programming model laid out in Section **??** in full, including explicit handler pools. It differs from our formal model in following Haskell's by-need evaluation strategy, which also means that concurrency in the library is *explicitly marked*, either through uses of a `fork` function or through asynchronous callbacks, which run in their own lightweight thread.

Implementing LVish as a Haskell library makes it possible to provide compile-time guarantees about determinism and quasi-determinism, because programs written using our library run in our `Par` monad and can therefore only perform LVish-sanctioned side effects. We take advantage of this fact by indexing `Par` computations with a phantom type that indicates their *determinism level*:

```
data Determinism = Det | QuasiDet
```

The `Par` type constructor has the following kind:[3]

```
Par :: Determinism → * → *
```

together with the following suite of `run` functions:

```
runPar   :: Par Det a → a
runParIO :: Par lvl a → IO a
```

[3] We are here using the `DataKinds` extension to Haskell to treat `Determinism` as a kind. In the full implementation, we include a second phantom type parameter to ensure that LVars cannot be used in multiple runs of the `Par` monad, in a manner analogous to how the ST monad prevents an `STRef` from being returned from `runST`.

```
runParThenFreeze :: DeepFrz a ⇒ Par Det a → FrzType a
```

The public library API ensures that if code uses `freeze`, it is marked as `QuasiDet`; thus, code that types as `Det` is guaranteed to be fully deterministic. While LVish code with an arbitrary determinism level `lvl` can be executed in the `IO` monad using `runParIO`, only `Det` code can be executed as if it were pure, since it is guaranteed to be free of visible side effects of nondeterminism. In the common case that `freeze` is only needed at the end of an otherwise-deterministic computation, `runParThenFreeze` runs the computation to completion, and then freezes the returned LVar, returning its exact value—and is guaranteed to be deterministic.[4]

AJT: We don't actually prove that freeze-free code is deterministic, but it should follow pretty easily from the proof of quasi-determinism. Perhaps we should claim it in the proof section? LK: Well, to do this "right" we would have to not just prove that freeze-free code is deterministic, but we'd have to prove that freeze-happens-last code is deterministic...

4.2.1. The Big Picture. We envision two parties interacting with our library. First, there are data structure authors, who use the library directly to implement a specific monotonic data structure (*e.g.*, a monotonically growing finite map). Second, there are application writers, who are clients of these data structures. Only the application writers receive a (quasi-)determinism guarantee; an author of a data structure is responsible for ensuring that the states their data structure can take on correspond to the elements of a lattice, and that the exposed interface to it corresponds to some use of `put`, `get`, `freeze`, and event handlers.

Thus, our library is focused primarily on *lattice-generic* infrastructure: the `Par` monad itself, a thread scheduler, support for blocking and signaling threads, handler pools, and event handlers. Since this infrastructure is unsafe (does not guarantee quasi-determinism), only data structure authors should import it, subsequently exporting a *limited* interface specific to their data structure. For finite maps, for instance, this interface might include key/value insertion, lookup, event handlers and pools, and freezing—along with higher-level abstractions built on top of these.

[4] The `DeepFrz` typeclass is used to perform freezing of nested LVars, producing values of frozen type (as given by the `FrzType` type function).

For this approach to scale well with available parallel resources, it is essential that the data structures themselves support efficient parallel access; a finite map that was simply protected by a global lock would force all parallel threads to sequentialize their access. Thus, we expect data structure authors to draw from the extensive literature on scalable parallel data structures, employing techniques like fine-grained locking and lock-free data structures [**25**]. Data structures that fit into the LVish model have a special advantage: because all updates must commute, it may be possible to avoid the expensive synchronization which *must* be used for non-commutative operations [**4**]. And in any case, monotonic data structures are usually much simpler to represent and implement than general ones.

4.2.2. Two Key Ideas.

Leveraging atoms. Monotonic data structures acquire "pieces of information" over time. In a lattice, the smallest such pieces are called the *atoms* of the lattice: they are elements not equal to $\bot$, but for which the only smaller element is $\bot$. Lattices for which every element is the lub of some set of atoms are called *atomistic*, and in practice most application-specific lattices used by LVish programs have this property—especially those whose elements represent collections.

In general, the LVish primitives allow arbitrarily large queries and updates to an LVar. But for an atomistic lattice, the corresponding data structure usually exposes operations that work at the atom level, semantically limiting `puts` to atoms, `gets` to threshold sets of atoms, and event sets to sets of atoms. For example, the lattice of finite maps is atomistic, with atoms consisting of all singleton maps (*i.e.*, all key/value pairs). The interface to a finite map usually works at the atom level, allowing addition of a new key/value pair, querying of a single key, or traversals (which we model as handlers) that walk over one key/value pair at a time.

Our implementation is designed to facilitate good performance for atomistic lattices by associating LVars with a set of *deltas* (changes), as well as a lattice. For atomistic lattices, the deltas are essentially just the atoms—for a set lattice, a delta is an element; for a map, a key/value pair. Deltas provide a compact way to represent a change to the lattice, allowing us to easily and efficiently communicate such changes between `puts` and `gets`/handlers.

Leveraging idempotence. While we have emphasized the commutativity of least upper bounds, they also provide another important property: *idempotence*, meaning that $d \sqcup d = d$ for any element d. In LVish terms, repeated `put`s or `freeze`s have no effect, and since these are the only way to modify the store, the result is that $e; e$ behaves the same as e for any LVish expression e. Idempotence has already been recognized as a useful property for work-stealing scheduling [**31**]: if the scheduler is allowed to occasionally duplicate work, it is possible to substantially save on synchronization costs. Since LVish computations are guaranteed to be idempotent, we could use such a scheduler (for now we use the standard Chase-Lev deque [**13**]). But idempotence also helps us deal with races between `put` and `get`/`addHandler`, as we explain below.

4.2.3. Representation Choices. Our library uses the following generic representation for LVars:

```
data LVar a d =
       LVar { state :: a,  status :: IORef (Status d) }
```

where the type parameter `a` is the (mutable) data structure representing the lattice, and `d` is the type of deltas for the lattice.[5] The `status` field is a mutable reference that represents the status bit:

```
data Status d = Frozen | Active (B.Bag (Listener d))
```

The status bit of an LVar is tied together with a bag of waiting *listeners*, which include blocked `get`s and handlers; once the LVar is frozen, there can be no further events to listen for.[6] The bag module (imported as `B`) supports atomic insertion and removal, and *concurrent* traversal:

```
put     :: Bag a → a → IO (Token a)
remove  :: Token a → IO ()
foreach :: Bag a → (a → Token a → IO ()) → IO ()
```

Removal of elements is done via abstract *tokens*, which are acquired by insertion or traversal. Updates may occur concurrently with a traversal, but are not guaranteed to be visible to it.

[5] For non-atomistic lattices, we take `a` and `d` to be the same type.

[6] In particular, with one atomic update of the flag we both mark the LVar as frozen and allow the bag to be garbage-collected.

A listener for an LVar is a pair of callbacks, one called when the LVar's lattice value changes, and the other when the LVar is frozen:

```
data Listener d = Listener {
  onUpd :: d → Token (Listener d) → SchedQ → IO (),
  onFrz ::      Token (Listener d) → SchedQ → IO () }
```

The listener is given access to its own token in the listener bag, which it can use to deregister from future events (useful for a get whose threshold has been passed). It is also given access to the CPU-local scheduler queue, which it can use to spawn threads.

4.2.4. The Core Implementation. Internally, the Par monad represents computations in continuation-passing style, in terms of their interpretation in the IO monad:

```
type ClosedPar = SchedQ → IO ()
type ParCont a = a → ClosedPar
mkPar :: (ParCont a → ClosedPar) → Par lvl a
```

The ClosedPar type represents ready-to-run Par computations, which are given direct access to the CPU-local scheduler queue. Rather than returning a final result, a completed ClosedPar computation must call the scheduler, sched, on the queue. A Par computation, on the other hand, completes by passing its intended result to its continuation—yielding a ClosedPar computation.

Figure 4.3 gives the implementation for three core lattice-generic functions: getLV, putLV, and freezeLV, which we explain next.

Threshold reading. The getLV function assists data structure authors in writing operations with get semantics. In addition to an LVar, it takes two *threshold functions*, one for global state and one for deltas. The *global threshold* gThresh is used to initially check whether the LVar is above some lattice value(s) by global inspection; the extra boolean argument gives the frozen status of the LVar. The *delta threshold* dThresh checks whether a particular update takes the state of the LVar above some lattice state(s). Both functions return Just r if the threshold has been passed, where r is the result of the read. To continue

```
getLV :: (LVar a d) → (a → Bool → IO (Maybe b))
                    → (d → IO (Maybe b)) → Par lvl b
getLV (LVar{state, status}) gThresh dThresh =
  mkPar $λk q →
    let onUpd d = unblockWhen (dThresh d)
        onFrz   = unblockWhen (gThresh state True)
        unblockWhen thresh tok q = do
          tripped ← thresh
          whenJust tripped $ λb → do
            B.remove tok
            Sched.pushWork q (k b)
    in do
      curStat ← readIORef status
      case curStat of
        Frozen → do   -- no further deltas can arrive!
          tripped ← gThresh state True
          case tripped of
            Just b  → exec (k b) q
            Nothing → sched q
        Active ls → do
          tok ← B.put ls (Listener onUpd onFrz)
          frz ← isFrozen status -- must recheck after
                                -- enrolling listener
          tripped ← gThresh state frz
          case tripped of
            Just b  → do
              B.remove tok  -- remove the listener
              k b q         -- execute our continuation
            Nothing → sched q


putLV :: LVar a d → (a → IO (Maybe d)) → Par lvl ()
putLV (LVar{state, status}) doPut = mkPar $ λk q → do
  Sched.mark q  -- publish our intent to modify the LVar
  delta   ← doPut state      -- possibly modify LVar
  curStat ← readIORef status -- read while q is marked
  Sched.clearMark q          -- retract our intent
  whenJust delta $ λd → do
```

our running example of finite maps with key/value pair deltas, we can use getLV internally to build the following getKey function that is exposed to application writers:

```
-- Wait for the map to contain a key; return its value
getKey key mapLV = getLV mapLV gThresh dThresh where
  gThresh m frozen = lookup key m
  dThresh (k,v) | k == key  = return (Just v)
                | otherwise = return Nothing
```

where lookup imperatively looks up a key in the underlying map.

The challenge in implementing getLV is the possibility that a *concurrent* put will push the LVar over the threshold. To cope with such races, getLV employs a somewhat pessimistic strategy: before doing anything else, it enrolls a listener on the LVar that will be triggered on any subsequent updates. If an update passes the delta threshold, the listener is removed, and the continuation of the get is invoked, with the result, in a new lightweight thread. *After* enrolling the listener, getLV checks the *global* threshold, in case the LVar is already above the threshold. If it is, the listener is removed, and the continuation is launched immediately; otherwise, getLV invokes the scheduler, effectively treating its continuation as a blocked thread.

By doing the global check only after enrolling a listener, getLV is sure not to miss any threshold-passing updates. It does *not* need to synchronize between the delta and global thresholds: if the threshold is passed just as getLV runs, it might launch the continuation twice (once via the global check, once via delta), but by idempotence this does no harm. This is a performance tradeoff: we avoid imposing extra synchronization on *all* uses of getLV at the cost of some duplicated work in a rare case. We can easily provide a second version of getLV that makes the alternative tradeoff, but as we will see below, idempotence plays an *essential* role in the analogous situation for handlers.

Putting and freezing. On the other hand, we have the putLV function, used to build operations with put semantics. It takes an LVar and an *update function* doPut that performs the put on the underlying data structure, returning a delta if the put actually changed the data structure. If there is such a delta, putLV subsequently invokes all currently-enrolled listeners on it.

The implementation of putLV is complicated by another race, this time with freezing. If the put is nontrivial (*i.e.*, it changes the value of the LVar), the race can be resolved in two ways. Either the freeze takes effect first, in which case the put must fault, or else the put takes effect first, in which case both succeed. Unfortunately, we have no means to both check the frozen status *and* attempt an update in a single atomic step.[7]

Our basic approach is to ask forgiveness, rather than permission: we eagerly perform the put, and only afterwards check whether the LVar is frozen. Intuitively, this is allowed because *if* the LVar is frozen, the Par computation is going to terminate with an exception—so the effect of the put cannot be observed!

Unfortunately, it is not enough to *just* check the status bit for frozenness afterward, for a rather subtle reason: suppose the put is executing concurrently with a get which it causes to unblock, and that the getting thread subsequently freezes the LVar. In this case, we *must* treat the freeze as if it happened after the put, because the freeze could not have occurred had it not been for the put. But, by the time putLV reads the status bit, it may already be set, which naively would cause putLV to fault.

To guarantee that such confusion cannot occur, we add a *marked* bit to each CPU scheduler state. The bit is set (using Sched.mark) prior to a put being performed, and cleared (using Sched.clear) only *after* putLV has subsequently checked the frozen status. On the other hand, freezeLV waits until it has observed a (transient!) clear mark bit on every CPU (using Sched.awaitClear) before actually freezing the LVar. This guarantees that any puts that *caused* the freeze to take place check the frozen status *before* the freeze takes place; additional puts that arrive concurrently may, of course, set a mark bit again after freezeLV has observed a clear status.

The proposed approach requires no barriers or synchronization instructions (assuming that the put on the underlying data structure acts as a memory barrier). Since the mark bits are per-CPU flags, they can generally be held in a core-local cache line in exclusive mode—meaning that marking and clearing them is extremely cheap. The only time that the busy flags can create cross-core communication is during freezeLV, which should only occur once per LVar computation.

[7] While we could require the underlying data structure to support such transactions, doing so would preclude the use of existing lock-free data structures, which tend to use a single-word compare-and-set operation to perform atomic updates. Lock-free data structures routinely outperform transaction-based data structures [**20**].

One final point: unlike getLV and putLV, which are polymorphic in their determinism level, freezeLV is statically QuasiDet.

Handlers, pools and quiescence. Given the above infrastructure, the implementation of handlers is relatively straightforward. We represent handler pools as follows:

```
data HandlerPool = HandlerPool {
  numCallbacks :: Counter,  blocked :: B.Bag ClosedPar }
```

where Counter is a simple counter supporting atomic increment, decrement, and checks for equality with zero.[8] We use the counter to track the number of currently-executing callbacks, which we can use to implement quiesce. A handler pool also keeps a bag of threads that are blocked waiting for the pool to reach a quiescent state.

We create a pool using newPool (of type Par lvl HandlerPool), and implement quiescence testing as follows:

```
quiesce :: HandlerPool → Par lvl ()
quiesce hp@(HandlerPool cnt bag) = mkPar $ λk q → do
  tok ← B.put bag (k ())
  quiescent ← poll cnt
  if quiescent then do B.remove tok; k () q
               else sched q
```

where the poll function indicates whether cnt is (transiently) zero. Note that we are following the same listener-enrollment strategy as in getLV, but with blocked acting as the bag of listeners.

Finally, addHandler has the following interface:

```
addHandler ::
     Maybe HandlerPool             -- Pool to enroll in
  → LVar a d                       -- LVar to listen to
  → (a → IO (Maybe (Par lvl ()))) -- Global callback
```

[8] One can use a high-performance *scalable non-zero indicator* [**17**] to implement Counter, but we have not yet done so.

```
  → (d → IO (Maybe (Par lvl ()))) -- Delta callback
  → Par lvl ()
```

As with getLV, handlers are specified using both global and delta threshold functions. Rather than returning results, however, these threshold functions return computations to run in a fresh lightweight thread if the threshold has been passed. Each time a callback is launched, the callback count is incremented; when it is finished, the count is decremented, and if zero, all threads blocked on its quiescence are resumed.

The implementation of addHandler is very similar to getLV, but there is one important difference: handler callbacks must be invoked for *all* events of interest, not just a single threshold. Thus, the Par computation returned by the global threshold function should execute its callback on, *e.g.*, all available atoms. Likewise, we do not remove a handler from the bag of listeners when a single delta threshold is passed; handlers listen continuously to an LVar until it is frozen. We might, for example, expose the following foreach function for a finite map:

```
foreach mh mapLV cb = addHandler mh lv gThresh dThresh
  where
    dThresh (k,v) = return (Just (cb k v))
    gThresh mp    = traverse mp (λ(k,v) → cb k v) mp
```

Here, idempotence really pays off: without it, we would have to synchronize to ensure that no callbacks are duplicated between the global threshold (which may or may not see concurrent additions to the map) and the delta threshold (which will catch all concurrent additions). We expect such duplications to be rare, since they can only arise when a handler is added concurrently with updates to an LVar.[9]

4.3. Evaluation: k-CFA Case Study

We now evaluate the expressiveness and performance of our Haskell LVish implementation. We expect LVish to particularly shine for: (1) parallelizing complicated algorithms on structured data that pose

[9] That said, it is possible to avoid all duplication by adding further synchronization, and in ongoing research, we are exploring various locking and timestamp schemes to do just that.

challenges for other deterministic paradigms, and (2) composing pipeline-parallel stages of computation (each of which may be internally parallelized). In this section, we focus on a case study that fits this mold: *parallelized control-flow analysis*. We discuss the process of porting a sequential implementation of k-CFA to a parallel implementation using LVish. In the companion technical report [**35**], we also give benchmarking results for LVish implementations of two graph-algorithm microbenchmarks: breadth-first search and maximal independent set.

4.3.1. k-CFA.

The k*-CFA* analyses provide a hierarchy of increasingly precise methods to compute the flow of values to expressions in a higher-order language. For this case study, we began with a simple, sequential implementation of k-CFA translated to Haskell from a version by Might [**32**].[10] The algorithm processes expressions written in a continuation-passing-style λ-calculus. It resembles a nondeterministic abstract interpreter in which stores map addresses to *sets* of abstract values, and function application entails a cartesian product between the operator and operand sets. Further, an address models not just a static variable, but includes a fixed k-size window of the calling history to get to that point (the k in k-CFA). Taken together, the current redex, environment, store, and call history make up the abstract state of the program, and the goal is to explore a graph of these abstract states. This graph-exploration phase is followed by a second, summarization phase that combines all the information discovered into one store.

Phase 1: breadth-first exploration. The following function from the original, sequential version of the algorithm expresses the heart of the search process:

```
explore :: Set State → [State] → Set State
explore seen [] = seen
explore seen (todo:todos)
   | todo ∈ seen = explore seen todos
   | otherwise    = explore (insert todo seen)
                             (toList (next todo) ++ todos)
```

[10] Haskell port by Max Bolingbroke: https://github.com/batterseapower/haskell-kata/blob/master/0CFA.hs.

This code uses idiomatic Haskell data types like Data.Set and lists. However, it presents a dilemma with respect to exposing parallelism. Consider attempting to parallelize explore using purely functional parallelism with futures—for instance, using the Strategies library [**29**]. An attempt to compute the next states in parallel would seem to be thwarted by the main thread rapidly forcing each new state to perform the seen-before check, todo ∈ seen. There is no way for independent threads to "keep going" further into the graph; rather, they check in with seen after one step.

We confirmed this prediction by adding a parallelism annotation: withStrategy (parBuffer 8 rseq) (next to The GHC runtime reported that 100% of created futures were "duds"—that is, the main thread forced them before any helper thread could assist. Changing rseq to rdeepseq exposed a small amount of parallelism—238/5000 futures were successfully executed in parallel—yielding no actual speedup.

Phase 2: summarization. The first phase of the algorithm produces a large set of states, with stores that need to be joined together in the summarization phase. When one phase of a computation produces a large data structure that is immediately processed by the next phase, lazy languages can often achieve a form of pipelining "for free". This outcome is most obvious with *lists*, where the head element can be consumed before the tail is computed, offering cache-locality benefits. Unfortunately, when processing a pure Set or Map in Haskell, such pipelining is not possible, since the data structure is internally represented by a balanced tree whose structure is not known until all elements are present. Thus phase 1 and phase 2 cannot overlap in the purely functional version—but they will in the LVish version, as we will see. In fact, in LVish we will be able to achieve partial deforestation in addition to pipelining. Full deforestation in this application is impossible, because the Sets in the implementation serve a memoization purpose: they prevent repeated computations as we traverse the graph of states.

4.3.2. Porting to the LVish Library.

Our first step was a *verbatim* port to LVish. We changed the original, purely functional program to allocate a new LVar for each new set or map value in the original code. This was done simply by changing two types, Set and Map, to their monotonic LVar counterparts, ISet and IMap. In particular, a store maps a program location (with context) onto a set of abstract values:

```
  import Data.LVar.Map as IM
```

```
import Data.LVar.Set as IS
type Store s = IMap Addr s (ISet s Value)
```

Next, we replaced allocations of containers, and map/fold operations over them, with the analogous operations on their LVar counterparts. The explore function above was replaced by the simple graph traversal function from Section ??! These changes to the program were mechanical, including converting pure to monadic code. Indeed, the key insight in doing the verbatim port to LVish was to consume LVars as if they were pure values, ignoring the fact that an LVar's contents are spread out over space and time and are modified through effects.

In some places the style of the ported code is functional, while in others it is imperative. For example, the summarize function uses nested forEach invocations to accumulate data into a store map:

```
summarize :: ISet s (State s) → Par d s (Store s)
summarize states = do
  storeFin ← newEmptyMap
  IS.forEach states   $ λ (State _ _ store _) →
    IM.forEach store  $ λ key vals →
      IS.forEach vals $ λ elmt  →
        IM.modify storeFin key (putInSet elmt)
  return storeFin
```

While this code can be read in terms of traditional parallel nested loops, it in fact creates a network of handlers that convey incremental updates from one LVar to another, in the style of data-flow networks. That means, in particular, that computations in a pipeline can *immediately* begin reading results from containers (*e.g.*, storeFin), long before their contents are final.

The LVish version of k-CFA contains 11 occurrences of forEach, as well as a few *cartesian-product* operations. The cartesian products serve to apply functions to combinations of all possible values that arguments may take on, greatly increasing the number of handler events in circulation. Moreover, chains of handlers registered with forEach result in cascades of events through six or more handlers. The

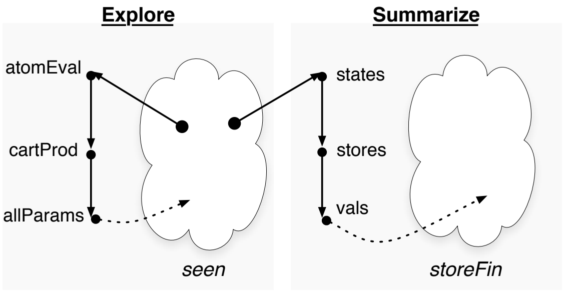


Figure 4.4. Simplified handler network for k-CFA. Exploration and summarization processes are driven by the same LVar. The triply-nested `forEach` calls in `summarize` become a chain of three handlers.

runtime behavior of these would be difficult to reason about. Fortunately, the programmer can largely ignore the temporal behavior of their program, since all LVish effects commute—rather like the way in which a lazy functional programmer typically need not think about the order in which thunks are forced at runtime.

Finally, there is an optimization benefit to using handlers. Normally, to flatten a nested data structure such as `[[[Int]]]` in a functional language, we would need to flatten one layer at a time and allocate a series of temporary structures. The LVish version avoids this; for example, in the code for `summarize` above, three `forEach` invocations are used to traverse a triply-nested structure, and yet the side effect in the innermost handler directly updates the final accumulator, `storeFin`.

Flipping the switch. The verbatim port uses LVars poorly: copying them repeatedly and discarding them without modification. This effect overwhelms the benefits of partial deforestation and pipelining, and the *verbatim* LVish port has a small performance overhead relative to the original. But not for long! The most clearly unnecessary operation in the verbatim port is in the `next` function. Like the pure code, it creates a fresh store to extend with new bindings as we take each step through the state space graph:

```
store' ← IM.copy store
```

Of course, a "copy" for an LVar is persistent: it is just a handler that forces the copy to receive everything the original does. But in LVish, it is also trivial to *entangle* the parallel branches of the search, allowing them to share information about bindings, simply by *not* creating a copy:

```
let store' = store
```

This one-line change speeds up execution by up to $25\times$ on a single thread, and the asynchronous, `ISet`-driven parallelism enables subsequent parallel speedup as well (up to $202\times$ total improvement over the purely functional version).

Figure 4.5 shows performance data for the "blur" benchmark drawn from a recent paper on k-CFA [**16**]. (We use $k = 2$ for the benchmarks in this section.) In general, it proved difficult to generate example inputs to k-CFA that took long enough to be candidates for parallel speedup. We were, however, able to "scale up" the blur benchmark by replicating the code N times, feeding one into the continuation argument for the next. Figure 4.5 also shows the results for one synthetic benchmark that managed to negate the benefits of our sharing approach, which is simply a long chain of 300 "not" functions (using a CPS conversion of the Church encoding for booleans). It has a small state space of large states with many variables (600 states and 1211 variables).

The role of lock-free data structures. As part of our library, we provide lock-free implementations of finite maps and sets based on concurrent skip lists [**25**].[11] We also provide reference implementations that use a nondestructive `Data.Set` inside a mutable container. Our scalable implementation is not yet carefully optimized, and at one and two cores, our lock-free k-CFA is 38% to 43% slower than the reference implementation on the "blur" benchmark. But the effect of scalable data structures is quite visible on a 12-core machine.[12] Without them, "blur" (replicated $8\times$) stops scaling and begins slowing down slightly after four cores. Even at four cores, variance is high in the reference implementation (min/max 0.96s / 1.71s over 7 runs). With lock-free structures, by contrast, performance steadily improves to a speedup of $8.14\times$ on 12 cores (0.64s at 67% GC productivity). Part of the benefit of LVish is to allow purely functional programs to make use of lock-free structures, in much the same way that the ST monad allows access to efficient in-place array computations.

TODO: Add benchmarks and case study from PLDI paper.

[11] In fact, this project is the first to incorporate *any* lock-free data structures in Haskell, which required solving some unique problems pertaining to Haskell's laziness and the GHC compiler's assumptions regarding referential transparency. But we lack the space to detail these improvements.

[12] Intel Xeon 5660; full machine details available at `https://portal.futuregrid.org/hardware/delta`.

LK: TODO: Ryan, we should try to make this legible when printed black and white.

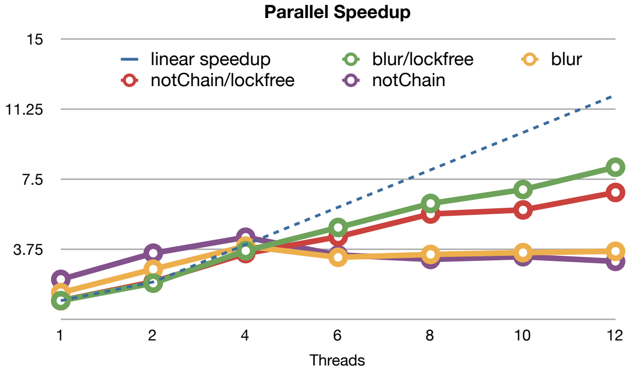


Figure 4.5. Parallel speedup for the "blur" and "notChain" benchmarks. Speedup is normalized to the sequential times for the *lock-free* versions (5.21s and 9.83s, respectively). The normalized speedups are remarkably consistent for the lock-free version between the two benchmarks. But the relationship to the original, purely functional version is quite different: at 12 cores, the lock-free LVish version of "blur" is $202\times$ faster than the original, while "notChain" is only $1.6\times$ faster, not gaining anything from sharing rather than copying stores due to a lack of fan-out in the state graph.

CHAPTER 5

Deterministic Threshold Queries of Distributed Data Structures

TODO: Revise this chapter.

5.1. Introduction

LK: Got rid of "reusedtext" markings for reused text from the WoDet paper, because we're not worried about those.

Distributed systems typically involve *replication* of data objects across a number of physical locations. Replication is of fundamental importance in such systems: it makes them more robust to data loss and allows for good data locality. But the well-known *CAP theorem* [**22, ?**] of distributed computing imposes a trade-off between *consistency*, in which every replica sees the same data, and *availability*, in which all data is available for both reading and writing by all replicas. *Highly available* distributed systems, such as Amazon's Dynamo key-value store [**15**], relax strong consistency in favor of *eventual consistency* [**48**], in which replicas need not agree at all times. Instead, updates execute at a particular replica and are sent to other replicas later. All updates eventually reach all replicas, albeit possibly in different orders. Informally speaking, eventual consistency says that if updates stop arriving, all replicas will *eventually* come to agree. RRN: Crystal clear so far, but I am now thinking in terms of sending sets of updates rather than sending state snapshots. Is this where you want me to be at? LK: The CRDT people would say that sending sets of updates is the "op-based" style and sending state snapshots is the "state-based" style. They would also say it doesn't really matter, since the two are equivalent. In this paper we're talking about the state-based style, so maybe we should revise this part. ...However, even in the state-based style, the "causal history" is the sets of operations that have taken place on the replicas, *not* the sets of the states they've been in! (Although in the concrete implementation, these sets of operations never get sent.)

Although giving up on strong consistency makes it possible for a distributed system to offer high availability, even an eventually consistent system must have some way of resolving conflicts between replicas that differ. One approach is to try to determine which replica was written most recently, then declare that replica the winner. But, even in the presence of a way to reliably synchronize clocks between replicas and hence reliably determine which replica was written most recently, having the last write win might not make sense from a *semantic* point of view. For instance, if a replicated object represents a set, then, depending on the application, the appropriate way to resolve a conflict between two replicas could be to take the set union of the replicas' contents. Such a conflict resolution policy might be more appropriate than a "last write wins" policy for, say, a object representing the contents of customer shopping carts for an online store [**15**].

5.1.1. Convergent replicated data types and eventual consistency. Implementing application-specific conflict resolution policies in an ad-hoc way for every application is tedious and error-prone.[1] Fortunately, we need not implement them in an ad-hoc way. Shapiro *et al.*'s *convergent replicated data types* (CvRDTs) [**43, 42**] provide a simple mathematical framework for reasoning about and enforcing the eventual consistency of replicated objects, based on viewing replica states as elements of a lattice and replica conflict resolution as the lattice's join operation.

In a CvRDT, the contents of a replica can only grow over time—that is, updates must be *inflationary* with respect to the given lattice—and replicas merge with remote replicas by taking the join of the remote state and the local state. CvRDTs offer a simple and theoretically-sound approach to eventual consistency. Still, even with CvRDTs, it is always possible to observe inconsistent *intermediate* states of replicated shared objects, and high availability requires that reads return a value immediately, even if that value is stale.

RRN: The "grow" description is appealing and intuitive. Probably good to leave it there for this paper. But it's good to keep in mind that in some lattices it may require fewer bits to represent higher states of the lattice rather than lower ones. For example, in a series of fork-join diamonds attached vertically, if a higher diamond has a smaller number of branches than a lower one. However, these are also the same

[1] Indeed, as the developers of Dynamo have noted [**15**], Amazon's shopping cart presents an anomaly whereby removed items may re-appear in the cart!

kinds of lattices where you can't do the threshold queries that you want. (Because you lose pairwise incompatibility for the sibling elements of the lower diamonds/fork-joins.) LK: Hmmm...we can say something about how we only mean "grow" in a "semantic" sense, not in the sense of actual number of bits it takes to represent a state. RRN: Very low priority issue though. More a note for our benefit.

5.1.2. Strong consistency at the query level. In practice, applications call for both strong consistency and high availability at different times [**?**], and increasingly, they support consistency choices at the granularity of individual queries, not that of the entire system. For example, the Amazon SimpleDB database service gives customers the choice between eventually consistent and strongly consistent read operations on a per-read basis [**?**].

Ordinarily, strong consistency is a global property: all replicas agree on the data. When we make consistency choices at a *per-query* granularity, though, a global strong consistency property need not hold. We define a *strongly consistent query* to be one that, if it returns a result x when executed at a replica i:

- will always return x on subsequent executions at i, and
- will *eventually* return x when executed at *any* replica, and will *block* until it does so.

That is, a strongly consistent query of a distributed data structure, if it returns, will return a result that is a *deterministic* function of all updates to the data structure in the entire distributed execution, regardless of when the query executes or which replica it occurs on.

5.1.3. Our contribution: bringing threshold queries to CvRDTs. As they are today, CvRDTs only support eventually consistent queries. We could get strong consistency by waiting until all replicas agree before allowing a query to return—but in practice, such agreement may never happen. In this paper, we offer an alternative approach to supporting strongly consistent queries that takes advantage of the existing lattice structure of CvRDTs and does not require waiting for all replicas to agree.

To do so we take inspiration from our previous work [**33, 36, 34**] on *LVars*, or lattice-based data structures for shared-memory deterministic parallelism. Like CvRDTs, LVars are data structures whose states are elements of an application-specific lattice, and whose contents can only grow with respect to the given lattice. Unlike CvRDTs, though, LVars make it impossible to observe the *order* of updates to their state. This is because LVar read operations are *threshold* reads: an attempt to read will block until the data structure's contents reach or surpass a particular "threshold" (which we explain in more detail in Section 5.2), and then return a deterministic result. The combination of inflationary writes and threshold reads allow LVars to serve as the basis for a *deterministic-by-construction* shared-memory parallel programming model: concurrent programs in which all shared data structures are LVars are guaranteed to produce a deterministic outcome on every run, regardless of parallel execution and schedule nondeterminism.LK: "Concurrent programs", but "parallel execution"—seems reasonable to me; will it make sense to other people? RRN: Sounds perfect to me. Readers for whom these are near synonyms will not blink, and readers who make the distinction should be happy too.

Although LVars and CvRDTs were developed independently, both models leverage the mathematical properties of join-semilattices to ensure that a property of the model holds—determinism in the case of LVars; eventual consistency in the case of CvRDTs. Our contribution in this paper is to bring LVar-style *threshold queries* to CvRDTs and show that threshold queries of CvRDTs are strongly consistent queries, according to the criteria given above. After reviewing the fundamentals of threshold queries (Section 5.2) and CvRDTs (Section 5.3), we introduce CvRDTs extended with threshold queries (Section 5.4) and prove that threshold queries in our extended model are strongly consistent queries (Section 5.5). That is, we show that a threshold query that returns an answer when executed on a replica will return the same answer every subsequent time that it is executed on that replica, and that executing that threshold query on a different replica will eventually return the same answer, and will block until it does so. RRN: This is pretty identically repeating what was in the definition in sec 1.2 less than one page earlier, no? LK: yep, just reiterating it – it might be too much. It is therefore impossible to observe different results from the same threshold query, whether at different times on the same replica, or whether on different replicas.

A preliminary version of some of the material in this paper appeared in a non-archival workshop [**?**]. LK: Things we do in this paper that we didn't do in the WoDet paper: we define what a strongly consistent query actually is; we define threshold queries in a more general way; we take into account the effect of potentially non-terminating threshold queries; we state and prove Theorem 2. Should we list out those things?

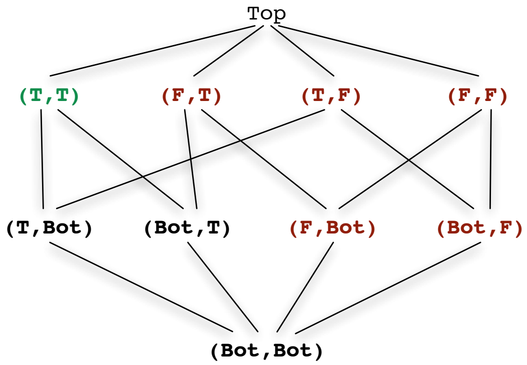


Figure 5.1. Lattice of states that an AndLV can take on. The five red states in the lattice correspond to a false result, and the one green to a true one.

RRN: Because wodet allows republication I do not think it is necessary at all to mention this workshop pub. Better to just focus on trumpeting the contributions here. LK: I dunno, I'd feel better mentioning it if we're reusing text from it, even though that's allowed.

RRN: I had mix feelings about them "enforcing" strong consistency... because they don't change the way writes and merges happen. (And if regular reads are still allowed...). What do you think of the above way of casting it? LK: Yeah, that was badly stated. This has been basically overhauled now; we're not talking about proving properties of the whole system, we're talking about proving properties of threshold queries.

LK: I commented out an old footnote about determinism vs. consistency because it's kind of out of date now. Determinism of a system and consistency of a system are different things, but in this paper we're distinguishing between consistency of a *system* and consistency of a *query*, and we're saying that a strongly consistent query is a deterministic query is a threshold query. We aren't talking about determinism of the whole system.

5.2. How threshold queries work

A *threshold query* is a way of reading the contents of a lattice-based data structure that allows only limited observations of the state of the data structure. It only returns a value when the data structure's state meets a certain (monotonic) criterion, or "threshold", and the value returned is the same regardless of how far above the threshold the data structure's state goes.

By a *lattice-based data structure*, we mean a data structure whose possible states are elements of a lattice[2], and that can only change over time in a way that is inflationary with respect to the lattice. Both CvRDTs [**43, 42**] and LVars [**33, 36**] are examples of lattice-based data structures. In this section, we illustrate threshold queries with an example before formally describing them in the context of CvRDTs.

5.2.1. An example: parallel "and". Consider a lattice-based data structure that stores the result of a parallel logical "and" operation. We will call this data structure an *AndLV*. For this example, we assume two inputs, called "left" and "right", each of which may be either T or F. To understand this example, it is sufficient to consider a single replica; in Section 5.4 we will go on to discuss replication and communication between replicas.

RRN: Tweaked this because I didn't want to imply in any way that this example doesn't work with multiple replicas. It's only for simplicity of exposition that we are holding off from talking about those. LK: sounds good.

We can represent the states an AndLV can take on as pairs (x,y), where each of x and y are T, F, or Bot. The Bot value, short for "bottom", is the state in which no input has yet been received, and so (Bot,Bot) is the least element of the lattice of states that our AndLV can take on, shown in Figure 5.1. An additional state, which we call Top, is the greatest element of the lattice; it represents the situation in which an error has occurred—if, for instance, one of the inputs writes T and then later changes its mind to F.

The result of the parallel "and" computation—if it completes successfully—will be either True or False, but it might also block indefinitely if not enough writes occur (say, if the left input is T and the right input never arrives), or it could end in an error state, discussed below. Each update to the lattice takes the form of a complete state, such as (T,Bot) to write the left input. RRN: This section didn't actually describe how write's happen - how is this? LK: oops, fixed now.

[2] We use "lattice" as a shorthand; formally, the "lattice" of states is a 4-tuple $(D, \sqsubseteq, \bot, \top)$, where D is a set, $\sqsubseteq$ is a partial order on D, $\bot$ is D's least element according to $\sqsubseteq$, $\top$ is D's greatest element, and every two elements in D have a least upper bound. Hence $(D, \sqsubseteq, \bot, \top)$ is really a *bounded join-semilattice* with a designated greatest element of $\top$.

The lattice induces a *join*, or least upper bound, operation on pairs of states; for instance, the join of (T,Bot) and (Bot,F) is (T,F), and the join of (T,Bot) and (F,Bot) is Top since the overlapping T and F values conflict. Importantly, whenever a write occurs, it updates the AndLV's state to the join of the incoming state and the current state. (With CvRDTs, this join is computed when replicas merge. In this example, though, we are dealing with only one replica, and updating to the join of the new state and the current state is sufficient to ensure that all writes are inflationary.)

LK: TODO: show the Haskell code in an appendix? I don't want to show it in the main part of the paper, not for this audience.

LK: TODO: Maybe we don't want typewriter font here at all, actually...

5.2.2. Threshold queries of an AndLV. Given that we want the result of a threshold query to be a deterministic function of the writes to a data structure—and not of the particular moment in time the query is made—what sorts of observations are safe to make of an AndLV? We cannot, for instance, test whether one or both inputs have been written at a particular point in time, because the result will depend on how the test is interleaved with the writes.

Instead, we can describe a *partial function* of the data structure's state that is undefined for all states except those that are at or above a certain *threshold* in the lattice. One way to describe such a function is to define a *threshold set* of sets of "activation" states. In the case of our AndLV, one of these sets of activation states is the set of states containing an F—that is, the set {(F,Bot), (Bot,F), (F,T), (T,F), (F,F)}. The elements of this set are shown in red in Figure 5.1. The other set of activation states singleton set {(T,T)}, shown in green in Figure 5.1. Therefore the entire threshold set is

$$\{\{\texttt{(F,Bot)}, \texttt{(Bot,F)}, \texttt{(F,T)}, \texttt{(T,F)}, \texttt{(F,F)}\}, \{\texttt{(T,T)}\}\}$$

The semantics of a threshold query is as follows: if a data structure's state reaches (or surpasses) any state or states in a particular set of activation states, the threshold query returns *the entire set* of activation states, regardless of which of those activation states was reached. If no state in any set of activation states has yet been reached, the threshold query will *block*; blocking corresponds to states on which the partial function is undefined.

In the case of our AndLV, as soon as either input writes an F, our threshold query will unblock and return the first set of activation states, that is, {(F,Bot), (Bot,F), (F,T), (T,F), (F,F)}. Hence AndLV has the expected "short-circuit" behavior and does not have to wait for a second input if the first input is F. If, on the other hand, both inputs write a T, the threshold query will unblock and return {(T,T)}.

In a real implementation, of course, the value returned from the query could be more meaningful to the client—for instance, we could return False instead of returning the set of activation states. However, doing so would only be a convenience, and the translation from {(F,Bot), (Bot,F), (F,T), (T,F), (F,F)} to False could just as easily take place on the client side. In either case, the result returned from the threshold query is the same regardless of *which* of the activation states caused it to unblock, and it is impossible for the client to tell whether the actual state of the lattice is, say, (T,F) or (F,F) or some other state containing F.

5.2.3. Pairwise incompatibility. In order for the behavior of a threshold query to be deterministic, it must be unblocked by a *unique* set of activation states in the threshold set. We ensure this by requiring that elements in a set of activation states must be *pairwise incompatible* with elements in every other set of activation states. That is, for all distinct sets of activation states Q and R in a given threshold set: $\forall q \in Q.\ \forall r \in R.\ q \sqcup r = \top$. LK: changed to inline math to save space. In our AndLV example, there are two distinct sets of activation states, so if we let $Q = \{$(T,T)$\}$ and $R = \{$(F,Bot), (Bot,F), (F,T), (T,F), (F,F)$\}$, the least upper bound of (T,T) and r must be Top, where r is any element of R. We can easily verify that this is the case. Furthermore, since the lattice of states that an AndLV can take on is finite, the join function can be verified to compute a least upper bound.

Why is pairwise incompatibility necessary? Consider the following (illegal) "threshold set" that does not meet the pairwise incompatibility criterion: $\{\{$(F,Bot), (Bot,F)$\}, \{$(T,Bot), (Bot,T)$\}\}$. LK: changed to inline math to save space. A threshold query corresponding to this so-called threshold set will unblock and return {(F,Bot), (Bot,F)} as soon as a state containing an F is reached, and {(T,Bot), (Bot,T)} as soon as a state containing a T is reached. The trouble with such a threshold query is that there exist states, such as (F,T) and (T,F), that could unblock either set of activation states. If the left input writes F and the right input writes T, and these writes occur in arbitrary order, then the threshold query will return a nondeterministic result, depending on the order in which the two writes arrive. But with the original, pairwise-incompatible threshold set we showed, the threshold query would deterministically return False—although if the T arrived first, the query would have to block until the F arrived, whereas if the F arrived first, it could unblock immediately. Hence threshold queries enforce consistency at the expense of availability, but it is still possible to do a "short-circuit" computation that unblocks as soon as an F is written.

The threshold set mechanism we describe in this section is part of the LVars programming model discussed in section 5.1; in fact, our AndLV example is precisely an LVar [**34**]. But the utility of threshold queries is not limited to LVars. In the following sections, we review the basics of the CvRDT model from the work of Shapiro *et al.*, then show how to add threshold queries to the CvRDT model, and prove that they are strongly consistent queries.

5.3. Background: CvRDTs and eventual consistency

Shapiro *et al.* [**43, 42**] define an *eventually consistent* object as one that meets three conditions. One of these conditions is the property of *convergence*: all correct replicas of an object at which the same updates have been delivered eventually have equivalent state. The other two conditions are *eventual delivery*, meaning that all replicas receive all update messages, and *termination*, meaning that all method executions terminate (we discuss methods in more detail below).

RRN: But we kind of break this termination property! The "microops" of individual "t" methods complete immediately, but at the polling layer the "macro-op" can block forever. Do we need to say something about how that is ok because the merges keep happening?

LK: I think that this is actually just fine, because all our proofs are about the inner layer, *not* the polling layer. The argument that we are making is that if the inner layer behaves in the way that we prove it does, then we get determinism by layering a polling layer on top of it – and the polling layer does not have to know anything about threshold sets or lattices or anything like that, so it's very conceptually simple.

Shapiro *et al*. further define a *strongly eventually consistent* (SEC) object as one that is eventually consistent and, in addition to being merely convergent, is *strongly convergent*, meaning that correct replicas at which the same updates have been delivered have equivalent state.[3] A *conflict-free replicated data type* (CRDT), then, is a data type (*i.e.*, a specification for an object) satisfying certain conditions that are sufficient to guarantee that the object is SEC. (The term "CRDT" is used interchangeably to mean a specification for an object, or an object meeting that specification.)

There are two "styles" of specifying a CRDT: *state-based*, also known as *convergent*[4]; or *operation-based* (or "op-based"), also known as *commutative*. CRDTs specified in the state-based style are called *convergent replicated data types*, abbreviated *CvRDTs*, while those specified in the op-based style are called *commutative replicated data types*, abbreviated *CmRDTs*. Of the two styles, we focus on the CvRDT style in this paper because CvRDTs are lattice-based data structures and therefore amenable to threshold queries described in Section 5.2—although, as Shapiro *et al*. show, CmRDTs can emulate CvRDTs and vice versa.

5.3.1. State-based objects. The Shapiro *et al*. model specifies a *state-based object* as a tuple (S, s^0, q, u, m), where S is a set of states, s^0 is the initial state, q is the *query method*, u is the *update method*, and m is the *merge method*. Objects are replicated across some finite number of processes, with one replica at each process, and each replica begins in the initial state s^0. The state of a local replica may be queried via the method q and updated via the method u. Methods execute locally, at a single replica, but the merge method m can merge the state from a remote replica with the local replica. The model assumes that each replica sends its state to the other replicas infinitely often, and that eventually every update reaches every replica, whether directly or indirectly.

[3] Strong eventual consistency is not to be confused with strong consistency: it is the combination of eventual consistency and strong convergence. Contrast with ordinary convergence, in which replicas only *eventually* have equivalent state. In a strongly convergent object, knowing that the same updates have been delivered to all correct replicas is sufficient to ensure that those replicas have equivalent state, whereas in an object that is merely convergent, there might be some further delay before all replicas agree.

[4]There is a potentially misleading terminology overlap here: the definitions of convergence and strong convergence above pertain not only to CvRDTs (where the C stands for "Convergent"), but to *all* CRDTs.

The assumption that replicas send their state to one another "infinitely often" refers not to the *frequency* of these state transmissions; rather; it says that, regardless of what event (such as an update, via the u method) occurs at a replica, a state transmission is guaranteed to occur after that event. We can therefore conclude that all updates eventually reach all replicas in a state-based object, meeting the "eventual delivery" condition discussed above. However, we still have no guarantee of strong convergence or even convergence. This is where Shapiro *et al.*'s notion of a CvRDT comes in: a state-based object that meets the criteria for a CvRDT is guaranteed to have the strong-convergence property.

A *state-based* or *convergent* replicated data type (CvRDT) is a state-based object equipped with a partial order $\leq$, written as a tuple $(S, \leq, s^0, q, u, m)$, that has the following properties:

- S forms a join-semilattice ordered by $\leq$.
- The merge method m computes the join of two states with respect to $\leq$.
- State is *inflationary* across updates: if u updates a state s to s', then $s \leq s'$.

Shapiro *et al.* show that a state-based object that meets the criteria for a CvRDT is strongly convergent. Therefore, given the eventual delivery guarantee that all state-based objects have, and given an additional assumption that all method executions terminate, a state-based object that meets the criteria for a CvRDT is SEC [**43**].

5.3.2. Discussion: the need for inflationary updates. LK: I think this is true, but I want someone else to check my reasoning. Although CvRDT updates are required to be inflationary, we note that it is not clear that inflationary updates are necessarily required for convergence. Consider, for example, a scenario in which replicas 1 and 2 both have the state $\{a, b\}$. Replica 1 updates its state to $\{a\}$, a non-inflationary update, and then sends its updated state to replica 2. Replica 2 merges the received state $\{a\}$ with $\{a, b\}$, and its state remains $\{a, b\}$. Then replica 2 sends its state back to replica 1; replica 1 merges $\{a, b\}$ with $\{a\}$, and its state becomes $\{a, b\}$. The non-inflationary update has been lost, and was, perhaps, nonsensical—but the replicas are nevertheless convergent.

However, once we introduce threshold queries of CvRDTs, as we will do in the following section, inflationary updates become *necessary* for the determinism of threshold queries. This is because a non-inflationary update could cause a threshold query that had been unblocked to block again, and so arbitrary interleaving of non-inflationary writes and threshold queries would lead to nondeterministic behavior. Therefore the requirement that updates be inflationary will not only be sensible, but actually crucial.

5.4. Adding threshold queries to CvRDTs

In Shapiro *et al.*'s CvRDT model, the query operation q reads the exact contents of its local replica, and therefore different replicas may see different states at the same time, if not all updates have been propagated yet. That is, it is possible to observe intermediate states of a CvRDT replica. Such intermediate observations are not possible with threshold queries. In this section, we show how to extend the CvRDT model to accommodate threshold queries.

5.4.1. Objects with threshold queries. Definition 5.1 extends Shapiro *et al.*'s definition of a state-based object with a threshold query method t:

Definition 5.1 (state-based object with threshold queries). A *state-based object with threshold queries* (henceforth *object*) is a tuple (S, s^0, q, t, u, m), where S is a set of states, $s^0 \in S$ is the initial state, q is a *query method*, t is a *threshold query method*, u is an *update method*, and m is a *merge method*.

In order to give a semantics to the threshold query method t, we need to formally define the notion of a threshold set described in Section 5.2:

Definition 5.2 (threshold set). A *threshold set with respect to a lattice* $(S, \leq)$ is a set $\mathcal{S} = \{S_a, S_b, \dots\}$ of one or more sets of *activation states*, where each set of activation states is a subset of S, the set of lattice elements, and where the following *pairwise incompatibility* property holds:

For all $S_a, S_b \in \mathcal{S}$, if $S_a \neq S_b$, then for all activation states $s_a \in S_a$ and for all activation states $s_b \in S_b$, $s_a \sqcup s_b = \top$, where $\sqcup$ is the join operation induced by $\leq$ and $\top$ is the greatest element of $(S, \leq)$.

In our model, we assume a finite set of n processes $p_1, \ldots, p_n$, and consider a single replicated object with one replica at each process, with replica i at process p_i. Processes may crash silently; we say that a non-crashed process is *correct*.

Every replica has initial state s^0. Methods execute at individual replicas, possibly updating that replica's state. The kth method execution at replica i is written $f_i^k(a)$, where k is ≥ 1 and f is either q, t, u, or m, and a is the arguments to f, if any. Methods execute sequentially at each replica. The state of replica i after the kth method execution at i is s_i^k. We say that states s and s' are equivalent, written $s \equiv s'$, if $q(s) = q(s')$.

5.4.2. Causal histories. An object's *causal history* is a record of all the updates that have happened at all replicas. The causal history does not track the order in which updates happened, merely that they did happen. The *causal history at replica i after execution k* is the set of all updates that have happened at replica i after execution k. Definition 5.3 updates Shapiro *et al.*'s definition of causal history for a state-based object to account for t (a trivial change, since execution of t does not change a replica's causal history):

Definition 5.3 (causal history). A *causal history* is a sequence $[c_1, \ldots, c_n]$, where c_i is a set of the updates that have occurred at replica i. Each c_i is initially $\emptyset$. If the kth method execution at replica i is:

- a query q or a threshold query t, then the causal history at replica i after execution k does not change: $c_i^k = c_i^{k-1}$.
- an update $u_i^k(a)$: then the causal history at replica i after execution k is $c_i^k = c_i^{k-1} \cup u_i^k(a)$.
- a merge $m_i^k(s_{i'}^{k'})$: then the causal history at replica i after execution k is the union of the local and remote histories: $c_i^k = c_i^{k-1} \cup c_{i'}^{k'}$.

We say that an update is *delivered at replica i* if it is in the causal history at replica i.

5.4.3. Threshold CvRDTs and the semantics of blocking. With the previous definitions in place, we can give the definition of a CvRDT that supports threshold queries:

LK: OK, it's a little confusing to use the letter t for the threshold query method, because op-based CRDTs use t for the "prepare-update" method. But, since this paper doesn't have op-based CRDTs, there's no ambiguity...I'm stealing it.

Definition 5.4 (CvRDT with threshold queries). A *convergent replicated data type with threshold queries* (henceforth *threshold CvRDT*) is an object equipped with a partial order $\leq$, written $(S, \leq, s^0, q, t, u, m)$, that has the following properties:

- S forms a join-semilattice ordered by $\leq$.
- S has a greatest element $\top$ according to $\leq$.
- The query method q takes no arguments and returns the local state.
- The threshold query method t takes a threshold set $\mathcal{S}$ as its argument, and has the following semantics: let $t_i^{k+1}(\mathcal{S})$ be the $k+1$th method execution at replica i, where $k \geq 0$. If, for some activation state s_a in some (unique) set of activation states $S_a \in \mathcal{S}$, the condition $s_a \leq s_i^k$ is met, $t_i^{k+1}(\mathcal{S})$ returns the set of activation states S_a. Otherwise, $t_i^{k+1}(\mathcal{S})$ returns the distinguished value block.
- The update method u takes a state as argument and updates the local state to it. RRN: Wait updates the local state to it? Or to the LUB of the input state and it? And if it's the latter, then do we need the next bullet, or is the inflationary property a consequence of this bullet? LK: It actually doesn't do a lub, it just does an inflationary update of any kind. the only lub that happens is with the merge method.
- State is *inflationary* across updates: if u updates a state s to s', then $s \leq s'$.
- The merge method m takes a remote state as its argument, computes the join of the remote state and the local state with respect to $\leq$, and updates the local state to the result.

and the q, t, u, and m methods have no side effects other than those listed above.

We use the block return value to model t's "blocking" behavior as a mathematical function with no intrinsic notion of running duration. When we say that a call to t "blocks", we mean that it immediately returns block, and when we say that a call to t "unblocks", we mean that it returns a set of activation states S_a.

Modeling blocking as a distinguished value introduces a new complication: we lose determinism, because a call to t at a particular replica may return either block or a set of activation states S_a, depending on the replica's state at the time it is called. However, we can conceal this nondeterminism with an additional layer over the nondeterministic API exposed by t. This additional layer simply *polls* t, calling it repeatedly until it returns a value other than block. Calls to t at a replica that are made by this "polling layer" count as method executions at that replica, and are arbitrarily interleaved with other method executions at the replica, including updates and merges. The polling layer itself need not do any computation other than checking to see whether t returns block or something else; in particular, the polling layer does not need to compare activation states to replica states, since that comparison is done by t itself. RRN: I'm afraid the prev sentence about polling/lvish gives the wrong impression, and a more nuanced one would take more space. So how about we nix it? The problem is that LVish is of course event driven. It doesn't sit around polling gets waiting for puts to happen. It only does anything when the put happens. And yet, the mapping of puts onto exact callbacks is not always perfectly precise. With an IVar it would be, but with an "IMap", the there's a callback registered on a particular key, and yet it might be polled every time a write is made to ANY key. That's just a limitation of the implementation currently – it can't do finer grain lists of guarded callbacks. More generally, some lvars really do *need* polling, yet they only need to poll when a write occurs.

The set of activation states S_a that a call to t returns when it unblocks is unique because of the pairwise incompatibility property described in Definition 5.2. The intuition behind pairwise incompatibility is that described in Section 5.2.3: without it, different orderings of updates could allow the same threshold query to unblock in different ways, introducing nondeterminism that would be observable beyond the polling layer.

5.4.4. Threshold CvRDTs are strongly eventually consistent.

LK: Hmmm. We don't have to do all this blathering about termination anymore, because now threshold queries actually do always return immediately!

We can define eventual consistency and strong eventual consistency exactly as Shapiro *et al*. do in their model. In the following definitions, a *correct replica* is a replica at a correct process, and the symbol $\Diamond$ means "eventually":

Definition 5.5 (eventual consistency (EC)). An object is *eventually consistent* (EC) if the following three conditions hold:

- *Eventual delivery*: An update delivered at some correct replica is eventually delivered at all correct replicas: $\forall i, j : f \in c_i \implies \Diamond f \in c_j$.
- *Convergence*: Correct replicas at which the same updates have been delivered eventually have equivalent state: $\forall i, j : c_i = c_j \implies \Diamond s_i \equiv s_j$.
- *Termination*: All method executions halt.

Definition 5.6 (strong eventual consistency (SEC)). An object is *strongly eventually consistent* (SEC) if it is eventually consistent and the following condition holds:

- *Strong convergence*: Correct replicas at which the same updates have been delivered have equivalent state: $\forall i, j : c_i = c_j \implies s_i \equiv s_j$.

Since we model blocking threshold queries with block, we need not be concerned with threshold queries not necessarily terminating. Determinism does *not* rule out queries that return block every time they are called (and would therefore cause the polling layer to block forever). However, we guarantee that if a threshold query returns block every time it is called during a complete run of the system, it will do so on *every* run of the system, regardless of scheduling. That is, it is not possible for a query to cause the polling layer to block forever on some runs, but not on others.LK: I changed the wording here from "execution" to "complete run of the system" to lessen confusion with individual method executions.

Finally, we can directly leverage Shapiro *et al*.'s SEC result for CvRDTs to show that a threshold CvRDT is SEC:

Theorem 5.1 (Strong Eventual Consistency of Threshold CvRDTs). *Assuming eventual delivery and termination, an object that meets the criteria for a threshold CvRDT is SEC.*

Proof. From Shapiro *et al.*, we have that an object that meets the criteria for a CvRDT is SEC [**43**]. Shapiro *et al.*'s proof also assumes that eventual delivery and termination hold for the object, and proves that strong convergence holds — that is, that given causal histories c_i and c_j for respective replicas i and j, that their states s_i and s_j are equivalent. The proof relies on the commutativity of the least upper bound operation. Since, according to our Definition 5.3, threshold queries do not affect causal history, we can leverage Shapiro *et al.*'s result to say that a threshold CvRDT is also SEC. □

RRN: Do we not need to grapple with the blocking forever behavior here with respect to reusing this result off the shelf? LK: right, we don't, because we aren't proving anything about the polling layer, just the inner CvRDT layer.

5.5. Determinism of threshold queries

Neither eventual consistency nor strong eventual consistency imply that *intermediate* results of the same query q on different replicas of a threshold CvRDT will be deterministic. For deterministic intermediate results, we must use the threshold query method t. We can show that t is deterministic *without* requiring that the same updates have been delivered at the replicas in question at the time that t runs.

In our previous work on LVars [**33, 36**], we showed that a threshold read of the contents of a shared-memory lattice-based data structure returns a deterministic result regardless of how that query is interleaved with updates to the data structure. Theorem 5.2 establishes that the same is true for threshold queries of *distributed, replicated* lattice-based data structures—namely, threshold CvRDTs.

Theorem 5.2 (Determinism of Threshold Queries). *Suppose a given threshold query t on a given threshold CvRDT returns a set of activation states S_a when executed at a replica i. Then, assuming eventual delivery and that no replica's state is ever $\top$ at any point in the execution:*

(1) *t will always return S_a on subsequent executions at i, and*
(2) *t will* eventually *return S_a when executed at* any *replica, and will* block *until it does so.*

Proof. Consider replica i of a threshold CvRDT $(S, \leq, s^0, q, t, u, m)$. Let $\mathcal{S}$ be a threshold set with respect to $(S, \leq)$. Consider a method execution $t_i^{k+1}(\mathcal{S})$ (*i.e.*, a threshold query that is the $k + 1$th method execution on replica i, with threshold set $\mathcal{S}$ as its argument) that returns some set of activation states $S_a \in \mathcal{S}$.

For part 1 of the theorem, we have to show that threshold queries with $\mathcal{S}$ as their argument will always return S_a on subsequent executions at i. That is, we have to show that, for all $k' > (k+1)$, the threshold query $t_i^{k'}(\mathcal{S})$ on i returns S_a.

Since $t_i^{k+1}(\mathcal{S})$ returns S_a, from Definition 5.4 we have that for some activation state $s_a \in S_a$, the condition $s_a \leq s_i^k$ holds. Consider arbitrary $k' > (k+1)$. Since state is inflationary across updates, we know that the state $s_i^{k'}$ after method execution k' is at least s_i^k. That is, $s_i^k \leq s_i^{k'}$. By transitivity of $\leq$, then, $s_a \leq s_i^{k'}$. Hence, by Definition 5.4, $t_i^{k'}(\mathcal{S})$ returns S_a.

For part 2 of the theorem, consider some replica j of $(S, \leq, s^0, q, t, u, m)$, located at process p_j. We are required to show that, for all $x \geq 0$, the threshold query $t_j^{x+1}(\mathcal{S})$ returns S_a eventually, and blocks until it does.[5] That is, we must show that, for all $x \geq 0$, there exists some finite $n \geq 0$ such that

- for all i in the range $0 \leq i \leq n-1$, the threshold query $t_j^{x+1+i}(\mathcal{S})$ returns block, and
- for all $i \geq n$, the threshold query $t_j^{x+1+i}(\mathcal{S})$ returns S_a.

Consider arbitrary $x \geq 0$. Recall that s_j^x is the state of replica j after the xth method execution, and therefore s_j^x is also the state of j when $t_j^{x+1}(\mathcal{S})$ runs. We have three cases to consider:

- $s_i^k \leq s_j^x$. (That is, replica i's state after the kth method execution on i is *at or below* replica j's state after the xth method execution on j.) Choose $n = 0$. We have to show that, for all $i \geq n$, the threshold query $t_j^{x+1+i}(\mathcal{S})$ returns S_a. Since $t_i^{k+1}(\mathcal{S})$ returns S_a, we know that there exists an $s_a \in S_a$ such that $s_a \leq s_i^k$. Since $s_i^k \leq s_j^x$, we have by transitivity of $\leq$ that $s_a \leq s_j^x$. Therefore, by Definition 5.4, $t_j^{x+1}(\mathcal{S})$ returns S_a. Then, by part 1 of the theorem, we have that subsequent executions $t_j^{x+1+i}(\mathcal{S})$ at replica j will also return S_a, and so the case holds. (Note that this case includes the possibility $s_i^k \equiv s^0$, in which no updates have executed at replica i.)

[5] The occurrences of $k+1$ and $x+1$ in this proof are an artifact of how we index method executions starting from 1, but states starting from 0. The initial state (of every replica) is s^0, and so s_i^k is the state of replica i after method execution k has completed at i.

- $s_i^k > s_j^x$. (That is, replica i's state after the kth method execution on i is *above* replica j's state after the xth method execution on j.)

  We have two subcases:

  – There exists some activation state $s'_a \in S_a$ for which $s'_a \leq s_j^x$. In this case, we choose $n = 0$. We have to show that, for all $i \geq n$, the threshold query $t_j^{x+1+i}(\mathcal{S})$ returns S_a. Since $s'_a \leq s_j^x$, by Definition 5.4, $t_j^{x+1}(\mathcal{S})$ returns S_a. Then, by part 1 of the theorem, we have that subsequent executions $t_j^{x+1+i}(\mathcal{S})$ at replica j will also return S_a, and so the case holds.

  – There is no activation state $s'_a \in S_a$ for which $s'_a \leq s_j^x$. Since $t_i^{k+1}(\mathcal{S})$ returns S_a, we know that there is some update $u_i^{k'}(a)$ in i's causal history, for some $k' < (k+1)$, that updates i from a state at or below s_j^x to s_i^k.[6] By eventual delivery, $u_i^{k'}(a)$ is eventually delivered at j. Hence some update or updates that will increase j's state from s_j^x to a state at or above some s'_a must reach replica j.[7]

    Let the $x+1+r$th method execution on j be the first update on j that updates its state to some $s_j^{x+1+r} \geq s'_a$, for some activation state $s'_a \in S_a$. Choose $n = r+1$. We have to show that, for all i in the range $0 \leq i \leq r$, the threshold query $t_j^{x+1+i}(\mathcal{S})$ returns block, and that for all $i \geq r+1$, the threshold query $t_j^{x+1+i}(\mathcal{S})$ returns S_a.

    For the former, since the $x+1+r$th method execution on j is the first one that updates its state to $s_j^{x+1+r} \geq s'_a$, we have by Definition 5.4 that for all i in the range $0 \leq i \leq r$, the threshold query $t_j^{x+1+i}(\mathcal{S})$ returns block.

    For the latter, since $s_j^{x+1+r} \geq s'_a$, by Definition 5.4 we have that $t_j^{x+1+r+1}(\mathcal{S})$ returns S_a, and by part 1 of the theorem, we have that for $i \geq r+1$, subsequent executions $t_j^{x+1+i}(\mathcal{S})$ at replica j will also return S_a, and so the case holds.

- $s_i^k \not\leq s_j^x$ and $s_j^x \not\leq s_i^k$. (That is, replica i's state after the kth method execution on i is *not comparable* to replica j's state after the xth method execution on j.) Similar to the previous case.

[6] We know that i's state was once at or below s_j^x, because i and j started at the same state s^0 and can both only grow. Hence the least that s_j^x can be is s^0, and we know that i was originally s^0 as well.

[7] We say "some update or updates" because the exact update $u_i^{k'}(a)$ may not be the update that causes the threshold query at j to unblock; a different update or updates could do it. Nevertheless, the existence of $u_i^{k'}(a)$ means that there is at least one update that will suffice to unblock the threshold query.

□

Although Theorem 5.2 must assume eventual delivery, it does *not* need to assume strong convergence or even ordinary convergence. It so happens that we have strong convergence as part of strong eventual consistency of threshold CvRDTs (by Theorem 5.1), but we do not need it to prove Theorem 5.2. In particular, there is no need for replicas to have the same state in order to return the same result from a particular threshold query. The replicas merely both need to be above an activation state from a unique set of activation states in the query's threshold set. Indeed, the replicas' states may in fact trigger *different* activation states from the same set of activation states.

Theorem 5.2's requirement that no replica's state is ever $\top$ rules out situations in which replicas disagree in a way that cannot be resolved normally. This would happen if, for instance, updates at two different replicas took their states to activation states from two distinct sets of activation states from the same threshold set. The join of the two replicas' states would be $\top$, which by eventual delivery would become the state of both replicas, but in the meantime, threshold queries of the two replicas would return different results. We rule out this situation by assuming that no replica's state goes to $\top$. (In a replicated version of the parallel "and" example from Section 5.2, this would happen if, for instance, one replica received a write of T on its left input while another received a write of F, also on its left input—a disagreement for which the only resolution is the error state, Top).

5.6. Related work

The extended CvRDT model we present in this paper is based on Shapiro *et al.*'s work on conflict-free replicated data types [**43, 42**], discussed in Section 5.3. Various other authors [**?, 10, 14**] have used lattices as a framework for establishing formal guarantees about eventually consistent systems and distributed programs. Burckhardt *et al.* [**?**] propose a formalism for eventual consistency based on graphs called *revision diagrams*. Burckhardt and Leijen [**10**] show that revision diagrams are semilattices, and Leijen, Burckhardt, and Fahndrich apply the revision diagrams approach to guaranteed-deterministic concurrent functional programming [**28**]. Conway *et al.*'s Bloom^L language for distributed programming leverages the lattice-based semantics of CvRDTs to guarantee confluence [**14**]. The concept of threshold queries comes from our previous work on the LVars model for lattice-based deterministic parallel programming [**33, 36, 34**].

As mentioned in Section 5.1, database services such as Amazon's SimpleDB [**?**] allow for both eventually consistent and strongly consistent reads, chosen at a per-query granularity. Terry *et al.*'s Pileus key-value store [**?**] takes the idea of mixing consistency levels further: instead of requiring the application developer to choose the consistency level of a particular query at development time, the system allows the developer to specify a service-level agreement that can dynamically adapt to changing network conditions, for instance. However, we are not aware of previous work on using lattice-based data structures as a foundation for both eventually consistent and strongly consistent queries.

5.7. Conclusion

In this paper we show how to extend CvRDTs with support for deterministic queries. Borrowing from our previous work on LVars for deterministic parallel programming, we propose *threshold queries*, which rather than returning the exact contents of a CvRDT, only reveal whether the contents have crossed a given "threshold" in the CvRDT's lattice. A threshold query blocks until the threshold is reached and then returns a deterministic result. We prove that a threshold query that returns a particular answer is guaranteed to return the same answer on subsequent queries of that replica, regardless of the replica's state. Moreover, executions of the same query on other replicas are guaranteed to eventually return the same answer, and to block until they do so. The threshold query technique generalizes to any lattice, and hence any CvRDT, allowing CvRDTs to support both eventually consistent and strongly consistent queries without waiting for all replicas to agree.

CHAPTER 6

Related Work

TODO: Revise this chapter.

LK: Following stuff is from my proposal.

Work on deterministic parallel programming models is long-standing. As discussed in Section 5.1, the LVars model builds on long traditions of work on parallel programming models based on monotonically-growing shared data structures, and it provides a framework for generalizing and unifying these existing approaches. In this section I describe some more recent contributions to the literature.

As we have seen, what deterministic parallel programming models have in common is that they all must do something to restrict access to mutable state shared among concurrent computations so that schedule nondeterminism cannot be observed. Depending on the model, restricting access to shared mutable state might involve disallowing sharing entirely [**39**], only allowing single assignments to shared references [**47, 3, 9**], allowing sharing only by a limited form of message passing [**26**], ensuring that concurrent accesses to shared state are disjoint [**7**], resolving conflicting updates after the fact [**28**], or some combination of these approaches. These constraints can be imposed at the language or API level, within a type system, or at runtime.

6.0.1. Deterministic Parallel Java (DPJ). DPJ [**7, 6**] is a deterministic language consisting of a system of annotations for Java code. A sophisticated region-based type system ensures that a mutable region of the heap is, essentially, passed linearly to an exclusive writer, thereby ensuring that the state accessed by concurrent threads is disjoint. DPJ does, however, provide a way to unsafely assert that operations commute with one another (using the `commuteswith` form) to enable concurrent mutation.

The LVars model differs from DPJ in that it allows overlapping shared state between threads as the default. Moreover, since LVar effects are already commutative, we avoid the need for `commuteswith` annotations. Finally, it is worth noting that while in DPJ, commutativity annotations have to appear in application-level code, in LVish only the data-structure author needs to write trusted code. The application programmer can run untrusted code that still enjoys a (quasi-)determinism guarantee, because only (quasi-)deterministic programs can be expressed as LVish `Par` computations.

More recently, Bocchino *et al*. [**8**] proposed a type and effect system that allows for the incorporation of nondeterministic sections of code in DPJ. The goal here is different from ours: while they aim to support *intentionally* nondeterministic computations such as those arising from optimization problems like branch-and-bound search, the quasi-determinism in LVish arises as a result of schedule nondeterminism.

6.0.2. FlowPools. Prokopec *et al*. [**40**] recently proposed a data structure with an API closely related to LVars extended with freezing and handlers: a FlowPool is a bag (that is, a multiset) that allows concurrent insertions but forbids removals, a `seal` operation that forbids further updates, and combinators like `foreach` that invoke callbacks as data arrives in the pool. To retain determinism, the `seal` operation requires explicitly passing the expected bag *size* as an argument, and the program will raise an exception if the bag goes over the expected size.

While this interface has a flavor similar to that of LVars, it lacks the ability to detect quiescence, which is crucial for expressing algorithms like graph traversal, and the `seal` operation is awkward to use when the structure of data is not known in advance. By contrast, the `freeze` operation on LVars does not require such advance knowledge, but moves the model into the realm of quasi-determinism. Another important difference is the fact that LVars are *data structure-generic*: both our formalism and our library support an unlimited collection of data structures, whereas FlowPools are specialized to bags.

6.0.3. Concurrent Revisions. The Concurrent Revisions (CR) [**28**] programming model uses isolation types to distinguish regions of the heap shared by multiple mutators. Rather than enforcing exclusive access in the style of DPJ, CR clones a copy of the state for each mutator, using a deterministic "merge function" for resolving conflicts in local copies at join points.

In CR, variables can be annotated as being shared between a "joiner" thread and a "joinee" thread. Unlike the least-upper-bound writes of LVars, CR merge functions are *not* necessarily commutative;

indeed, the default CR merge function is "joiner wins". Determinism is enforced by the programming model allowing the programmer to specify which of two writing threads should prevail, regardless of the order in which those writes arrive, and the states that a shared variable can take on need not form a lattice. Still, semilattices turn up in the metatheory of CR: in particular, Burckhardt and Leijen [**10**] show that, for any two vertices in a CR revision diagram, there exists a *greatest common ancestor* state that can be used to determine what changes each side has made—an interesting duality with our model (in which any two LVar states have a lub).LK: TODO: Write to them and ask them if it's a join-semilattice or a meet-semilattice!

Although versioned variables in CR could model lattice-based data structures—if they used least upper bound as their merge function for conflicts—the programming model nevertheless differs from the LVars model in that effects only become visible at the end of parallel regions, as opposed to the asynchronous communication within parallel regions that the LVars model allows. This semantics precludes the use of traditional lock-free data structures for representing versioned variables.

6.0.4. Bloom and Bloom^L. The Bloom language for distributed database programming guarantees eventual consistency for distributed data collections that are updated monotonically. The initial formulation of Bloom [**2**] had a notion of monotonicity based on set inclusion, analogous to the store ordering used in the proof of determinism for the (IVar-based) CnC system [**9**]. More recently, Conway *et al.* [**14**] generalized Bloom to a more flexible lattice-parameterized system, Bloom^L, in a manner analogous to our generalization from IVars to LVars. Bloom^L combines ideas from CRDTs with *monotonic logic*, resulting in a lattice-parameterized, confluent language that is a close relative of LVish. A monotonicity analysis pass rules out programs that would perform non-monotonic operations on distributed data collections, whereas in the LVars model, monotonicity is enforced by the API presented by LVars. Another difference between Bloom(^{L}) and the LVars model is that the former does not have a notion of quasi-determinism.LK: TODO: make sure this is the case—I think there might be some sort of way to unsafely peek in Bloom, but it's ruled out by the CALM analysis. Finally, since LVish is implemented as a Haskell library (whereas Bloom(^{L}) is implemented as a domain-specific language embedded in Ruby), we can rely on Haskell's static type system for fine-grained effect tracking and monadic encapsulation of LVar effects.

LK: Following stuff is from the FHPC paper, and might get axed.

Work on deterministic parallel programming models is long-standing. In addition to the single-assignment and KPN models already discussed, here we consider a few recent contributions to the literature.

Deterministic Parallel Java (DPJ). DPJ [**6**] is a deterministic language consisting of a system of annotations for Java code. A sophisticated region-based type system ensures that a mutable region of the heap is, essentially, passed linearly to an exclusive writer. While a linear type system or region system like that of DPJ could be used to enforce single assignment statically, accommodating λ_{LVar}'s semantics would involve parameterizing the type system by the application-specific lattice.

DPJ also provides a way to unsafely assert that operations commute with one another (using the `commuteswith` form) to enable concurrent mutation. However, DPJ does not provide direct support for modeling message-passing (*e.g.*, KPNs) or asynchronous communication within parallel regions. RRN: DOUBLE CHECK THIS. Finally, a key difference between the λ_{LVar} model and DPJ is that λ_{LVar} retains determinism by restricting *what* can be read or written, rather than by restricting the semantics of reads and writes themselves.

Concurrent Revisions. The Concurrent Revisions (CR) [**28**] programming model uses isolation types to distinguish regions of the heap shared by multiple mutators. Rather than enforcing exclusive access, CR clones a copy of the state for each mutator, using a deterministic policy for resolving conflicts in local copies. The management of shared variables in CR is tightly coupled to a fork-join control structure, and the implementation of these variables is similar to reduction variables in other languages (*e.g.*, Cilk *hyperobjects*). CR charts an important new area in the deterministic-parallelism design space, but one that differs significantly from λ_{LVar}. CR could be used to model similar types of data structures—if versioned variables used least upper bound as their merge function for conflicts—but effects would only become visible at the end of parallel regions, rather than λ_{LVar}'s asynchronous communication within parallel regions.

Bloom and Bloom^L. LK: Augh, I really want to mention CRDTs, but no room!

In the distributed systems literature, *eventually consistent* systems [**49**] leverage the idea of monotonicity to guarantee that, for instance, nodes in a distributed database eventually agree. The Bloom language for distributed database programming [**2**] guarantees eventual consistency for distributed data collections that are updated monotonically. The initial formulation of Bloom had a notion of monotonicity based on *set containment*, analogous to the store ordering for single-assignment languages given in Definition **??**. However, recent work by Conway *et al.* [**14**] generalizes Bloom to a more flexible lattice-parameterized system, Bloom^L, in a manner analogous to our generalization from IVars to LVars. Bloom^L comes with a library of built-in lattice types and also allows for users to implement their own lattice types as Ruby classes. Although Conway *et al.* do not give a proof of eventual consistency for Bloom^L, our determinism result for λ_{LVar} suggests that their generalization is indeed safe. Moreover, although the goals of Bloom^L differ from those of LVars, we believe that Bloom^L bodes well for programmers' willingness to use lattice-based data structures, and lattice-parameterized languages based on them, to address real-world programming challenges.

LK: Following stuff is from the POPL paper, and might get axed.

6.1. Related Work

Monotonic data structures: traditional approaches. LVish builds on two long traditions of work on parallel programming models based on monotonically-growing shared data structures:

- In *Kahn process networks* (KPNs) [**26**], as well as in the more restricted *synchronous data flow* systems [**27**], a network of processes communicate with each other through blocking FIFO channels with ever-growing *channel histories*. Each process computes a sequential, monotonic function from the history of its inputs to the history of its outputs, enabling pipeline parallelism. KPNs are the basis for deterministic stream-processing languages such as StreamIt [**23**].
- In parallel *single-assignment languages* [**47**], "full/empty" bits are associated with heap locations so that they may be written to at most once. Single-assignment locations with blocking read semantics—that is, *IVars* [**3**]—have appeared in Concurrent ML as `SyncVars` [**41**]; in the Intel Concurrent Collections system [**9**]; in languages and libraries for high-performance computing, such as Chapel

> [12] and the Qthreads library [50]; and have even been implemented in hardware in Cray MTA machines [5]. Although most of these uses incorporate IVars into already-nondeterministic programming environments, Haskell's Par monad [30]—on which our LVish implementation is based—uses IVars in a deterministic-by-construction setting, allowing user-created threads to communicate through IVars without requiring IO, so that such communication can occur anywhere inside pure programs.

LVars are general enough to subsume both IVars and KPNs: a lattice of channel histories with a prefix ordering allows LVars to represent FIFO channels that implement a Kahn process network, whereas an LVar with "empty" and "full" states (where $empty < full$) behaves like an IVar, as we described in Section **??**. Hence LVars provide a framework for generalizing and unifying these two existing approaches to deterministic parallelism.

Deterministic Parallel Java (DPJ). DPJ [7, 6] is a deterministic language consisting of a system of annotations for Java code. A sophisticated region-based type system ensures that a mutable region of the heap is, essentially, passed linearly to an exclusive writer, thereby ensuring that the state accessed by concurrent threads is disjoint. DPJ does, however, provide a way to unsafely assert that operations commute with one another (using the `commuteswith` form) to enable concurrent mutation.

LVish differs from DPJ in that it allows overlapping shared state between threads as the default. Moreover, since LVar effects are already commutative, we avoid the need for `commuteswith` annotations. Finally, it is worth noting that while in DPJ, commutativity annotations have to appear in application-level code, in LVish only the data-structure author needs to write trusted code. The application programmer can run untrusted code that still enjoys a (quasi-)determinism guarantee, because only (quasi-)deterministic programs can be expressed as LVish Par computations.

More recently, Bocchino *et al*. [8] proposed a type and effect system that allows for the incorporation of nondeterministic sections of code in DPJ. The goal here is different from ours: while they aim to support *intentionally* nondeterministic computations such as those arising from optimization problems like branch-and-bound search, LVish's quasi-determinism arises as a result of schedule nondeterminism.

FlowPools. Prokopec *et al.* [**40**] recently proposed a data structure with an API closely related to ideas in LVish: a FlowPool is a bag that allows concurrent insertions but forbids removals, a `seal` operation that forbids further updates, and combinators like `foreach` that invoke callbacks as data arrives in the pool. To retain determinism, the `seal` operation requires explicitly passing the expected bag *size* as an argument, and the program will raise an exception if the bag goes over the expected size.

While this interface has a flavor similar to LVish, it lacks the ability to detect quiescence, which is crucial for supporting examples like graph traversal, and the `seal` operation is awkward to use when the structure of data is not known in advance. By contrast, our `freeze` operation is more expressive and convenient, but moves the model into the realm of quasi-determinism. Another important difference is the fact that LVish is *data structure-generic*: both our formalism and our library support an unlimited collection of data structures, whereas FlowPools are specialized to bags. Nevertheless, FlowPools represent a “sweet spot” in the deterministic parallel design space: by allowing handlers but not general freezing, they retain determinism while improving on the expressivity of the original LVars model. We claim that, with our addition of handlers, LVish generalizes FlowPools to add support for arbitrary lattice-based data structures.

Concurrent Revisions. The Concurrent Revisions (CR) [**28**] programming model uses isolation types to distinguish regions of the heap shared by multiple mutators. Rather than enforcing exclusive access, CR clones a copy of the state for each mutator, using a deterministic “merge function” for resolving conflicts in local copies at join points. Unlike LVish’s least-upper-bound writes, CR merge functions are *not* necessarily commutative; the default CR merge function is “joiner wins”. Still, semilattices turn up in the metatheory of CR: in particular, Burckhardt and Leijen [**10**] show that, for any two vertices in a CR revision diagram, there exists a *greatest common ancestor* state which can be used to determine what changes each side has made—an interesting duality with our model (in which any two LVar states have a lub).

While CR could be used to model similar types of data structures to LVish—if versioned variables used least upper bound as their merge function for conflicts—effects would only become visible at the end of parallel regions, rather than LVish’s asynchronous communication within parallel regions. This precludes the use of traditional lock-free data structures as a representation.

Conflict-free replicated data types. In the distributed systems literature, *eventually consistent* systems based on *conflict-free replicated data types* (CRDTs) [**43**] leverage lattice properties to guarantee that replicas in a distributed database eventually agree. Unlike LVars, CRDTs allow intermediate states to be observed: if two replicas are updated independently, reads of those replicas may disagree until a (least-upper-bound) merge operation takes place. Various data-structure-specific techniques can ensure that non-monotonic updates (such as removal of elements from a set) are not lost.

The Bloom^L language for distributed database programming [**14**] combines CRDTs with *monotonic logic*, resulting in a lattice-parameterized, confluent language that is a close relative of LVish. A monotonicity analysis pass rules out programs that would perform non-monotonic operations on distributed data collections, whereas in LVish, monotonicity is enforced by the LVar API.

Future work will further explore the relationship between LVars and CRDTs: in one direction, we will investigate LVar-based data structures inspired by CRDTs that support non-monotonic operations; in the other direction, we will investigate the feasibility and usefulness of LVar threshold reads in a distributed setting.

TODO: Add stuff from PLDI paper, maybe?

TODO: Add stuff from DISC submission.

CHAPTER 7

Conclusion

TODO: Revise this chapter.

LK: THe following text is from the FHPC paper conclusion.

As single-assignment languages and Kahn process networks demonstrate, monotonicity serves as the foundation of deterministic parallelism. Taking monotonicity as a starting point, the LVars model generalizes single assignment to monotonic multiple assignment parameterized by an application-specific lattice. Combining monotonic writes with threshold reads yields a provably deterministic shared-state parallel programming model that generalizes and unifies a class of languages suitable for asynchronous parallel applications.

TODO: Dump in conclusion material from other papers.

Bibliography

[1] Breadth-First Search, Parallel Boost Graph Library. URL `http://www.boost.org/doc/libs/1_51_0/libs/graph_parallel/doc/html/breadth_first_search.html`.

[2] P. Alvaro, N. Conway, J. Hellerstein, and W. R. Marczak. Consistency analysis in Bloom: a CALM and collected approach. In *CIDR*, 2011.

[3] Arvind, R. S. Nikhil, and K. K. Pingali. I-structures: data structures for parallel computing. *ACM Trans. Program. Lang. Syst.*, 11(4), Oct. 1989.

[4] H. Attiya, R. Guerraoui, D. Hendler, P. Kuznetsov, M. M. Michael, and M. Vechev. Laws of order: expensive synchronization in concurrent algorithms cannot be eliminated. In *POPL*, 2011.

[5] D. A. Bader and K. Madduri. Designing multithreaded algorithms for breadth-first search and st-connectivity on the Cray MTA-2. In *ICPP*, 2006.

[6] R. L. Bocchino, Jr., V. S. Adve, S. V. Adve, and M. Snir. Parallel programming must be deterministic by default. In *HotPar*, 2009.

[7] R. L. Bocchino, Jr., V. S. Adve, D. Dig, S. V. Adve, S. Heumann, R. Komuravelli, J. Overbey, P. Simmons, H. Sung, and M. Vakilian. A type and effect system for deterministic parallel Java. In *OOPSLA*, 2009.

[8] R. L. Bocchino, Jr. et al. Safe nondeterminism in a deterministic-by-default parallel language. In *POPL*, 2011.

[9] Z. Budimlić, M. Burke, V. Cavé, K. Knobe, G. Lowney, R. Newton, J. Palsberg, D. Peixotto, V. Sarkar, F. Schlimbach, and S. Taşirlar. Concurrent Collections. *Sci. Program.*, 18(3-4), Aug. 2010.

[10] S. Burckhardt and D. Leijen. Semantics of concurrent revisions. In *ESOP*, 2011.

[11] M. M. T. Chakravarty, R. Leshchinskiy, S. Peyton Jones, G. Keller, and S. Marlow. Data Parallel Haskell: A status report. In *DAMP*, 2007.

[12] B. L. Chamberlain, D. Callahan, and H. P. Zima. Parallel programmability and the Chapel language. *International Journal of High Performance Computing Applications*, 21(3), 2007.

[13] D. Chase and Y. Lev. Dynamic circular work-stealing deque. In *SPAA*, 2005.

[14] N. Conway, W. Marczak, P. Alvaro, J. M. Hellerstein, and D. Maier. Logic and lattices for distributed programming. In *SOCC*, 2012.

[15] G. DeCandia, D. Hastorun, M. Jampani, G. Kakulapati, A. Lakshman, A. Pilchin, S. Sivasubramanian, P. Vosshall, and W. Vogels. Dynamo: Amazon's highly available key-value store. In *SOSP*, 2007.

[16] C. Earl, I. Sergey, M. Might, and D. Van Horn. Introspective pushdown analysis of higher-order programs. In *ICFP*, 2012.

[17] F. Ellen, Y. Lev, V. Luchangco, and M. Moir. SNZI: Scalable NonZero Indicators. In *PODC*, 2007.

[18] M. Felleisen, R. B. Findler, and M. Flatt. *Semantics Engineering with PLT Redex*. The MIT Press, 1st edition, 2009.

[19] M. Fluet, M. Rainey, J. Reppy, and A. Shaw. Implicitly-threaded parallelism in Manticore. In *ICFP*, 2008.

[20] K. Fraser. *Practical lock-freedom*. PhD thesis, 2004.

[21] M. Frigo, C. E. Leiserson, and K. H. Randall. The implementation of the Cilk-5 multithreaded language. In *PLDI*, 1998.

[22] S. Gilbert and N. Lynch. Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. *SIGACT News*, 33(2), June 2002.

[23] M. I. Gordon, W. Thies, M. Karczmarek, J. Lin, A. S. Meli, C. Leger, A. A. Lamb, J. Wong, H. Hoffman, D. Z. Maze, and S. Amarasinghe. A stream compiler for communication-exposed architectures. In *ASPLOS*, 2002.

[24] S. Herhut, R. L. Hudson, T. Shpeisman, and J. Sreeram. River trail: A path to parallelism in javascript. In *OOPSLA*, 2013.

[25] M. Herlihy and N. Shavit. *The Art of Multiprocessor Programming*. Morgan Kaufmann, 2008.

[26] G. Kahn. The semantics of a simple language for parallel programming. In J. L. Rosenfeld, editor, *Information processing*. North Holland, Amsterdam, Aug. 1974.

[27] E. Lee and D. Messerschmitt. Synchronous data flow. *Proceedings of the IEEE*, 75(9):1235–1245, 1987.

[28] D. Leijen, M. Fahndrich, and S. Burckhardt. Prettier concurrency: purely functional concurrent revisions. In *Haskell*, 2011.

[29] S. Marlow, P. Maier, H.-W. Loidl, M. K. Aswad, and P. Trinder. Seq no more: better strategies for parallel Haskell. In *Haskell*, 2010.

[30] S. Marlow, R. Newton, and S. Peyton Jones. A monad for deterministic parallelism. In *Haskell*, 2011.

[31] M. M. Michael, M. T. Vechev, and V. A. Saraswat. Idempotent work stealing. In *PPoPP*, 2009.

[32] M. Might. k-CFA: Determining types and/or control-flow in languages like Python, Java and Scheme. http://matt.might.net/articles/implementation-of-kcfa-and-0cfa/.

[33] Lindsey Kuper and R. R. Newton. LVars: lattice-based data structures for deterministic parallelism. In *FHPC*, 2013.

[34] Lindsey Kuper, A. Todd, S. Tobin-Hochstadt, and R. R. Newton. Taming the parallel effect zoo: Extensible deterministic parallelism with LVish. In *PLDI*, 2014 (to appear).

[35] Lindsey Kuper, A. Turon, N. R. Krishnaswami, and R. R. Newton. Freeze after writing: Quasi-deterministic parallel programming with LVars. Technical Report TR710, Indiana University, Nov. 2013. URL `http://www.cs.indiana.edu/cgi-bin/techreports/TRNNN.cgi?trnum=TR710%` fi.

[36] Lindsey Kuper, A. Turon, N. R. Krishnaswami, and R. R. Newton. Freeze after writing: Quasi-deterministic parallel programming with LVars. In *POPL*, 2014.

[37] R. R. Newton and I. L. Newton. PhyBin: binning trees by topology. *PeerJ*, 1:e187, Oct. 2013.

[38] R. S. Nikhil. Id language reference manual, 1991.

[39] S. L. Peyton Jones, R. Leshchinskiy, G. Keller, and M. M. T. Chakravarty. Harnessing the multicores: Nested data parallelism in Haskell. In *FSTTCS*, 2008.

[40] A. Prokopec, H. Miller, T. Schlatter, P. Haller, and M. Odersky. FlowPools: a lock-free deterministic concurrent dataflow abstraction. In *LCPC*, 2012.

[41] J. H. Reppy. *Concurrent Programming in ML*. Cambridge University Press, Cambridge, England, 1999.

[42] M. Shapiro, N. Preguiça, C. Baquero, and M. Zawirski. A comprehensive study of Convergent and Commutative Replicated Data Types. Technical Report RR-7506, INRIA, Jan. 2011.

[43] M. Shapiro, N. Preguiça, C. Baquero, and M. Zawirski. Conflict-free replicated data types. In *SSS*, 2011.

[44] D. Spoonhower, G. E. Blelloch, P. B. Gibbons, and R. Harper. Beyond nested parallelism: tight bounds on work-stealing overheads for parallel futures. In *SPAA*, 2009.

[45] S.-J. Sul and T. L. Williams. A randomized algorithm for comparing sets of phylogenetic trees. In *APBC*, 2007.

[46] D. Terei, D. Mazières, S. Marlow, and S. Peyton Jones. Safe haskell. In *Haskell*, 2012.

[47] L. G. Tesler and H. J. Enea. A language design for concurrent processes. In *AFIPS*, 1968 (Spring).

[48] W. Vogels. Eventually consistent. *Commun. ACM*, 52(1), Jan. 2009.

[49] W. Vogels. Eventually consistent. *Commun. ACM*, 52(1), Jan. 2009.

[50] K. B. Wheeler, R. C. Murphy, and D. Thain. Qthreads: An API for programming with millions of lightweight threads, 2008.

APPENDIX A

Proofs

A.1. Proof of Lemma 2.1

Proof. By induction on the derivation of $\langle S;\ e\rangle \hookrightarrow \langle S';\ e'\rangle$, by cases on the last rule in the derivation.

- Case E-Eval-Ctxt:

  Given: $\langle S;\ E[e]\rangle \hookrightarrow \langle S';\ E[e']\rangle$.

  To show: $S \sqsubseteq_S S'$.

  From the premise of E-Eval-Ctxt, $\langle S;\ e\rangle \hookrightarrow \langle S';\ e'\rangle$.

  Hence by IH, $S \sqsubseteq_S S'$, as we were required to show.

- Case E-Beta:

  Immediate by the definition of $\sqsubseteq_S$, since S does not change.

- Case E-New:

  Given: $\langle S;\ \texttt{new}\rangle \hookrightarrow \langle S[l \mapsto \bot];\ l\rangle$.

  To show: $S \sqsubseteq_S S[l \mapsto \bot]$.

  By Definition 2.2, we have to show that $\mathit{dom}(S) \subseteq \mathit{dom}(S[l \mapsto \bot])$ and that for all $l' \in \mathit{dom}(S)$, $S(l') \sqsubseteq (S[l \mapsto \bot])(l')$.

  By definition, a store update operation on S can only either update an existing binding in S or extend S with a new binding. Hence $\mathit{dom}(S) \subseteq \mathit{dom}(S[l \mapsto \bot])$.

  From the side condition of E-New, $l \notin \mathit{dom}(S)$. Hence $S[l \mapsto \bot]$ adds a new binding for l in S.

  Hence $S[l \mapsto \bot]$ does not update any existing bindings in S.

  Hence, for all $l' \in \mathit{dom}(S), S(l') \sqsubseteq (S[l \mapsto \bot])(l')$.

  Therefore $S \sqsubseteq_S S[l \mapsto \bot]$, as required.

- Case E-Put:

  Given: $\langle S;\ \texttt{put}\ l\ d_2\rangle \hookrightarrow \langle S[l \mapsto d_1 \sqcup d_2];\ \texttt{()}\rangle$.

To show: $S \sqsubseteq_S S[l \mapsto d_1 \sqcup d_2]$.

By Definition 2.2, we have to show that $dom(S) \subseteq dom(S[l \mapsto d_1 \sqcup d_2])$ and that for all $l' \in dom(S)$, $S(l') \sqsubseteq (S[l \mapsto d_1 \sqcup d_2])(l')$.

By definition, a store update operation on S can only either update an existing binding in S or extend S with a new binding. Hence $dom(S) \subseteq dom(S[l \mapsto p_2])$.

From the premises of E-Put, $S(l) = d_1$. Therefore $l \in dom(S)$.

Hence $S[l \mapsto d_1 \sqcup d_2]$ updates the existing binding for l in S from d_1 to $d_1 \sqcup d_2$.

By the definition of $\sqcup$, $d_1 \sqsubseteq (d_1 \sqcup d_2)$. $S[l \mapsto d_1 \sqcup d_2]$ does not update any other bindings in S, hence, for all $l' \in dom(S), S(l') \sqsubseteq (S[l \mapsto d_1 \sqcup d_2])(l')$.

Hence $S \sqsubseteq_S S[l \mapsto d_1 \sqcup d_2]$, as required.

- Case E-Put-Err:

  Given: $\langle S;\ \texttt{put}\ l\ d_2 \rangle \hookrightarrow$ **error**.

  By the definition of **error**, **error** $= \langle \top_S;\ e \rangle$ for any e.

  To show: $S \sqsubseteq_S \top_S$.

  Immediate by the definition of $\sqsubseteq_S$.

- Case E-Get:

  Immediate by the definition of $\sqsubseteq_S$, since S does not change.

□

A.2. Proof of Lemma 2.2

Proof. Consider arbitrary S'' such that S'' is non-conflicting with $\langle S;\ e \rangle \hookrightarrow \langle S';\ e' \rangle$ and $S' \sqcup_S S'' \neq \top_S$.

To show: $\langle S \sqcup_S S'';\ e \rangle \hookrightarrow \langle S' \sqcup_S S'';\ e' \rangle$.

The proof is by induction on the derivation of $\langle S;\ e \rangle \hookrightarrow \langle S';\ e' \rangle$, by cases on the last rule in the derivation. In every case we may assume that $\langle S';\ e' \rangle \neq$ **error**. Since $\langle S';\ e' \rangle \neq$ **error**, we do not need to consider the E-Put-Err rule.

- Case E-Eval-Ctxt:

Given: $\langle S;\ E[e]\rangle \hookrightarrow \langle S';\ E[e']\rangle$.

To show: $\langle S \sqcup_S S'';\ E[e]\rangle \hookrightarrow \langle S' \sqcup_S S'';\ E[e']\rangle$.

From the premise of E-Eval-Ctxt, we have that $\langle S;\ e\rangle \hookrightarrow \langle S';\ e'\rangle$.

Therefore, by IH, we have that $\langle S \sqcup_S S'';\ e\rangle \hookrightarrow \langle S' \sqcup_S S'';\ e'\rangle$.

Therefore, by E-Eval-Ctxt, we have that $\langle S \sqcup_S S'';\ E[e]\rangle \hookrightarrow \langle S' \sqcup_S S'';\ E[e']\rangle$, as we were required to show.

- Case E-Beta:

  Given: $\langle S;\ (\lambda x.\, e)\ v\rangle \hookrightarrow \langle S;\ e[x := v]\rangle$.

  To show: $\langle S \sqcup_S S'';\ (\lambda x.\, e)\ v\rangle \hookrightarrow \langle S \sqcup_S S'';\ e[x := v]\rangle$.

  Immediate by E-Beta.

- Case E-New:

  Given: $\langle S;\ \texttt{new}\rangle \hookrightarrow \langle S[l \mapsto \bot];\ l\rangle$.

  To show: $\langle S \sqcup_S S'';\ \texttt{new}\rangle \hookrightarrow \langle (S[l \mapsto \bot]) \sqcup_S S'';\ l\rangle$.

  By E-New, we have that $\langle S \sqcup_S S'';\ \texttt{new}\rangle \hookrightarrow \langle (S \sqcup_S S'')[l' \mapsto \bot];\ l'\rangle$, where $l' \notin \mathit{dom}(S \sqcup_S S'')$.

  By assumption, S'' is non-conflicting with $\langle S;\ \texttt{new}\rangle \hookrightarrow \langle S[l \mapsto \bot];\ l\rangle$.

  Therefore $l \notin \mathit{dom}(S'')$.

  From the side condition of E-New, $l \notin \mathit{dom}(S)$.

  Therefore $l \notin \mathit{dom}(S \sqcup_S S'')$.

  Therefore, in $\langle (S \sqcup_S S'')[l' \mapsto \bot];\ l'\rangle$, we can α-rename l' to l,

  resulting in $\langle (S \sqcup_S S'')[l \mapsto \bot];\ l\rangle$.

  Therefore $\langle S \sqcup_S S'';\ \texttt{new}\rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto \bot];\ l\rangle$.

  Note that:

$$\begin{aligned}
(S \sqcup_S S'')[l \mapsto \bot] &= S[l \mapsto \bot] \sqcup_S S''[l \mapsto \bot] \\
&= S \sqcup_S [l \mapsto \bot] \sqcup_S S'' \sqcup_S [l \mapsto \bot] \\
&= S \sqcup_S [l \mapsto \bot] \sqcup_S S'' \\
&= S[l \mapsto \bot] \sqcup_S S''.
\end{aligned}$$

  Therefore $\langle S \sqcup_S S'';\ \texttt{new}\rangle \hookrightarrow \langle S[l \mapsto \bot] \sqcup_S S'';\ l\rangle$, as we were required to show.

- Case E-Put:

Given: $\langle S;\ \texttt{put}\ l\ d_2\rangle \hookrightarrow \langle S[l \mapsto d_2];\ \texttt{()}\rangle$.

To show: $\langle S \sqcup_S S'';\ \texttt{put}\ l\ d_2\rangle \hookrightarrow \langle S[l \mapsto d_2] \sqcup_S S'';\ \texttt{()}\rangle$.

We will first show that

$\langle S \sqcup_S S'';\ \texttt{put}\ l\ d_2\rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto d_2];\ \texttt{()}\rangle$

and then show why this is sufficient.

We proceed by cases on l:

- $l \notin \mathit{dom}(S'')$:

  By assumption, $S[l \mapsto d_2] \sqcup_S S'' \neq \top_S$.

  By Lemma 2.1, $S \sqsubseteq_S S[l \mapsto d_2]$.

  Hence $S \sqcup_S S'' \neq \top_S$.

  Therefore, by Definition 2.3, $(S \sqcup_S S'')(l) = S(l)$.

  From the premises of E-Put, $S(l) = d_1$.

  Hence $(S \sqcup_S S'')(l) = d_1$.

  From the premises of E-Put, $d_2 = d_1 \sqcup d_2$ and $d_2 \neq \top$.

  Therefore, by E-Put, we have: $\langle S \sqcup_S S'';\ \texttt{put}\ l\ d_2\rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto d_2];\ \texttt{()}\rangle$.

- $l \in \mathit{dom}(S'')$:

  By assumption, $S[l \mapsto d_2] \sqcup_S S'' \neq \top_S$.

  By Lemma 2.1, $S \sqsubseteq_S S[l \mapsto d_2]$.

  Hence $S \sqcup_S S'' \neq \top_S$.

  Therefore $(S \sqcup_S S'')(l) = S(l) \sqcup S''(l)$.

  From the premises of E-Put, $S(l) = d_1$.

  Hence $(S \sqcup_S S'')(l) = d_1'$, where $d_1 \sqsubseteq d_1'$.

  From the premises of E-Put, $d_2 = d_1 \sqcup d_2$.

  Let $d_2' = d_1' \sqcup d_2$.

  Hence $d_2 \sqsubseteq d_2'$.

  By assumption, $S[l \mapsto d_2] \sqcup_S S'' \neq \top_S$.

  Therefore, by Definition 2.3, $d_2 \sqcup_S S''(l) \neq \top$.

Note that:

$$\begin{aligned}
\top \neq d_2 \sqcup_S S''(l) \\
&= d_1 \sqcup d_2 \sqcup S''(l) \\
&= S(l) \sqcup d_2 \sqcup S''(l) \\
&= S(l) \sqcup S''(l) \sqcup d_2 \\
&= (S \sqcup_S S'')(l) \sqcup d_2 \\
&= d_1' \sqcup d_2 \\
&= d_2'.
\end{aligned}$$

Hence $d_2' \neq \top$.

Hence $(S \sqcup_S S'')(l) = d_1'$ and $d_2' = d_1' \sqcup d_2$ and $d_2' \neq \top$.

Therefore, by E-Put we have: $\langle S \sqcup_S S''; \texttt{put}\ l\ d_2 \rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto d_2']; \texttt{()} \rangle$.

LK: If we really wanted to be pedantic here, we'd actually prove that the stores are equal. I'm assuming that if I can show that $(S \sqcup_S S'')[l \mapsto d_2']$ and $(S \sqcup_S S'')[l \mapsto d_2]$ bind l to the same value, then it will be obvious that they're equal.

Note that:

$$\begin{aligned}
((S \sqcup_S S'')[l \mapsto d_2'])(l) &= (S \sqcup_S S'')(l) \sqcup ([l \mapsto d_2'])(l) \\
&= d_1' \sqcup d_2' \\
&= d_1' \sqcup d_1' \sqcup d_2 \\
&= d_1' \sqcup d_2
\end{aligned}$$

and

$$\begin{aligned}
((S \sqcup_S S'')[l \mapsto d_2])(l) &= (S \sqcup_S S'')(l) \sqcup ([l \mapsto d_2])(l) \\
&= d_1' \sqcup d_2 \\
&= d_1' \sqcup d_1 \sqcup d_2 \\
&= d_1' \sqcup d_2 && \text{(since } d_1 \sqsubseteq d_1'\text{).}
\end{aligned}$$

Therefore $(S \sqcup_S S'')[l \mapsto d_2'] = (S \sqcup_S S'')[l \mapsto d_2]$.

Therefore, $\langle S \sqcup_S S'';\ \texttt{put}\ l\ d_2 \rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto d_2];\ \texttt{()} \rangle$.

Note that:

$$\begin{aligned}(S \sqcup_S S'')[l \mapsto d_2] &= S[l \mapsto d_2] \sqcup_S S''[l \mapsto d_2] \\ &= S \sqcup_S [l \mapsto d_2] \sqcup_S S'' \sqcup_S [l \mapsto d_2] \\ &= S \sqcup_S [l \mapsto d_2] \sqcup_S S'' \\ &= S[l \mapsto d_2] \sqcup_S S''.\end{aligned}$$

Therefore $\langle S \sqcup_S S'';\ \texttt{put}\ l\ d_2 \rangle \hookrightarrow \langle S[l \mapsto d_2] \sqcup_S S'';\ \texttt{()} \rangle$, as we were required to show.

- Case E-Get:

  Given: $\langle S;\ \texttt{get}\ l\ T \rangle \hookrightarrow \langle S;\ d_2 \rangle$.

  To show: $\langle S \sqcup_S S'';\ \texttt{get}\ l\ T \rangle \hookrightarrow \langle S \sqcup_S S'';\ d_2 \rangle$.

  From the premises of E-Get, $S(l) = d_1$ and *incomp*(T) and $d_2 \in T$ and $d_2 \sqsubseteq d_1$.

  By assumption, $S \sqcup_S S'' \neq \top_S$.

  Hence $(S \sqcup_S S'') = d_1'$, where $d_1 \sqsubseteq d_1'$.

  By the transitivity of $\sqsubseteq$, $d_2 \sqsubseteq d_1'$.

  Hence, $S(l) = d_1'$ and *incomp*(T) and $d_2 \in T$ and $d_2 \sqsubseteq d_1'$.

  Therefore, by E-Get,

  $\langle S \sqcup_S S'';\ \texttt{get}\ l\ T \rangle \hookrightarrow \langle S \sqcup_S S'';\ d_2 \rangle$,

  as we were required to show.

□

A.3. Proof of Lemma 2.3

Proof. Consider arbitrary S'' such that S'' is non-conflicting with $\langle S;\ e \rangle \hookrightarrow \langle S';\ e' \rangle$ and $S' \sqcup_S S'' = \top_S$.

To show: $\langle S \sqcup_S S'';\ e \rangle \hookrightarrow$ **error**.

The proof is by induction on the derivation of $\langle S;\, e\rangle \hookrightarrow \langle S';\, e'\rangle$, by cases on the last rule in the derivation. In every case we may assume that $\langle S';\, e'\rangle \neq$ **error**. Since $\langle S';\, e'\rangle \neq$ **error**, we do not need to consider the E-Put-Err rule.

- Case E-Eval-Ctxt:

  Given: $\langle S;\, E[e]\rangle \hookrightarrow \langle S';\, E[e']\rangle$.

  To show: $\langle S \sqcup_S S'';\, E[e]\rangle \hookrightarrow^i$ **error**, where $i \leq 1$.

  From the premise of E-Eval-Ctxt, we have that $\langle S;\, e\rangle \hookrightarrow \langle S';\, e'\rangle$.

  Therefore, by IH, we have that $\langle S \sqcup_S S'';\, e\rangle \hookrightarrow^{i'}$ **error**, where $i' \leq 1$.

  We proceed by cases on i':

  - $i' = 0$:

    In this case, $\langle S \sqcup_S S'';\, e\rangle =$ **error**.

    Hence, by the definition of **error**, $S \sqcup_S S'' = \top_S$.

    Hence $\langle S \sqcup_S S'';\, E[e]\rangle =$ **error**.

    Hence $\langle S \sqcup_S S'';\, E[e]\rangle \hookrightarrow^i$ **error**, with $i = 0$.

  - $i' = 1$:

    In this case, $\langle S \sqcup_S S'';\, e\rangle \hookrightarrow$ **error**.

    By the definition of **error**, **error** $= \langle \top_S;\, e''\rangle$ for any e''.

    Hence $\langle S \sqcup_S S'';\, e\rangle \hookrightarrow \langle \top_S;\, e''\rangle$.

    Hence, by E-Eval-Ctxt, $\langle S \sqcup_S S'';\, E[e]\rangle \hookrightarrow \langle \top_S;\, E[e'']\rangle$.

    By the definition of **error**, $\langle \top_S;\, E[e'']\rangle =$ **error**.

    Hence $\langle S \sqcup_S S'';\, E[e]\rangle \hookrightarrow$ **error**.

    Hence $\langle S \sqcup_S S'';\, E[e]\rangle \hookrightarrow^i$ **error**, with $i = 1$.

- Case E-Beta:

  Given: $\langle S;\, (\lambda x.\, e)\, v\rangle \hookrightarrow \langle S;\, e[x := v]\rangle$.

  To show: $\langle S \sqcup_S S'';\, (\lambda x.\, e)\, v\rangle \hookrightarrow^i$ **error**, where $i \leq 1$.

  By assumption, $S \sqcup_S S'' = \top_S$.

  Hence, by the definition of **error**, $\langle S \sqcup_S S'';\, (\lambda x.\, e)\, v\rangle =$ **error**.

  Hence $\langle S \sqcup_S S'';\, (\lambda x.\, e)\, v\rangle \hookrightarrow^i$ **error**, with $i = 0$.

- Case E-New:

  Given: $\langle S;\ \texttt{new}\rangle \hookrightarrow \langle S[l \mapsto \bot];\ l\rangle$.

  To show: $\langle S \sqcup_S S'';\ \texttt{new}\rangle \hookrightarrow^i$ **error**, where $i \leq 1$.

  By E-New, $\langle S \sqcup_S S'';\ \texttt{new}\rangle \hookrightarrow \langle (S \sqcup_S S'')[l' \mapsto \bot];\ l'\rangle$, where $l' \notin \mathit{dom}(S \sqcup_S S'')$.

  By assumption, S'' is non-conflicting with $\langle S;\ \texttt{new}\rangle \hookrightarrow \langle S[l \mapsto \bot];\ l\rangle$.

  Therefore $l \notin \mathit{dom}(S'')$.

  From the side condition of E-New, $l \notin \mathit{dom}(S)$.

  Therefore $l \notin \mathit{dom}(S \sqcup_S S'')$.

  Therefore, in $\langle (S \sqcup_S S'')[l' \mapsto \bot];\ l'\rangle$, we can α-rename l' to l,

  resulting in $\langle (S \sqcup_S S'')[l \mapsto \bot];\ l\rangle$.

  Therefore $\langle S \sqcup_S S'';\ \texttt{new}\rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto \bot];\ l\rangle$.

  By assumption, $S[l \mapsto \bot] \sqcup_S S'' = \top_S$.

  Note that:

  $$\begin{aligned}
  \top_S &= S[l \mapsto \bot] \sqcup_S S'' \\
  &= S \sqcup_S [l \mapsto \bot] \sqcup_S S'' \\
  &= S \sqcup_S S'' \sqcup_S [l \mapsto \bot] \\
  &= (S \sqcup_S S'') \sqcup_S [l \mapsto \bot] \\
  &= (S \sqcup_S S'')[l \mapsto \bot].
  \end{aligned}$$

  Hence $\langle S \sqcup_S S'';\ \texttt{new}\rangle \hookrightarrow \langle \top_S;\ l\rangle$.

  Hence, by the definition of **error**, $\langle S \sqcup_S S'';\ \texttt{new}\rangle \hookrightarrow$ **error**.

  Hence $\langle S \sqcup_S S'';\ \texttt{new}\rangle \hookrightarrow^i$ **error**, with $i = 1$.

- Case E-Put:

  Given: $\langle S;\ \texttt{put}\ l\ d_2\rangle \hookrightarrow \langle S[l \mapsto d_2];\ \texttt{()}\rangle$.

  To show: $\langle S \sqcup_S S'';\ \texttt{put}\ l\ d_2\rangle \hookrightarrow^i$ **error**, where $i \leq 1$.

  We proceed by cases on $S \sqcup_S S''$:

  - $S \sqcup_S S'' = \top_S$:

    In this case, by the definition of **error**, $\langle S \sqcup_S S'';\ \texttt{put}\ l\ d_2\rangle =$ **error**.

    Hence $\langle S \sqcup_S S'';\ \texttt{put}\ l\ d_2\rangle \hookrightarrow^i$ **error**, with $i = 0$.

- $S \sqcup_S S'' \neq \top_S$:

  From the premises of E-Put, we have that $S(l) = d_1$.

  Hence $(S \sqcup_S S'')(l) = d_1'$, where $d_1 \sqsubseteq d_1'$.

  We show that $d_1' \sqcup d_2 = \top$, as follows:

  By assumption, $S[l \mapsto d_2] \sqcup_S S'' = \top_S$.

  Hence, by Definition 2.3, there exists some $l' \in \mathit{dom}(S[l \mapsto d_2]) \cap \mathit{dom}(S'')$ such that $(S[l \mapsto d_2])(l') \sqcup S''(l') = \top$.

  Now case on l':

  - $l' \neq l$:

    In this case, $(S[l \mapsto d_2])(l') = S(l')$.

    Since $(S[l \mapsto d_2])(l') \sqcup S''(l') = \top$, we then have that $S(l') \sqcup S''(l') = \top$.

    However, this is a contradiction since $S \sqcup_S S'' \neq \top_S$.

    Hence this case cannot occur.

  - $l' = l$:

    Then $(S[l \mapsto d_2])(l) \sqcup S''(l) = \top$.

    Note that:

$$\begin{aligned}\top &= (S[l \mapsto d_2])(l) \sqcup S''(l)\\ &= d_2 \sqcup S''(l)\\ &= d_1 \sqcup d_2 \sqcup S''(l)\\ &= S(l) \sqcup d_2 \sqcup S''(l)\\ &= S(l) \sqcup S''(l) \sqcup d_2\\ &= (S \sqcup_S S'')(l) \sqcup d_2\\ &= d_1' \sqcup d_2.\end{aligned}$$

    Hence $d_1' \sqcup d_2 = \top$.

    Hence, by E-Put-Err, $\langle S \sqcup_S S''; \texttt{put}\ l\ d_2 \rangle \hookrightarrow$ **error**.

    Hence $\langle S \sqcup_S S''; \texttt{put}\ l\ d_2 \rangle \hookrightarrow^i$ **error**, with $i = 1$.

- Case E-Get:

Given: $\langle S;\ \texttt{get}\ l\ T \rangle \hookrightarrow \langle S;\ d_2 \rangle$.

To show: $\langle S \sqcup_S S'';\ \texttt{get}\ l\ T \rangle \hookrightarrow^i$ **error**, where $i \leq 1$.

By assumption, $S \sqcup_S S'' = \top_S$.

Hence, by the definition of **error**, $\langle S \sqcup_S S'';\ \texttt{get}\ l\ T \rangle =$ **error**.

Hence $\langle S \sqcup_S S'';\ \texttt{get}\ l\ T \rangle \hookrightarrow^i$ **error**, with $i = 0$.

□

A.4. Proof of Lemma 2.4

TODO: Figure out if we even actually need this property, and if so, what to do here. If we do need it, then do we only need to handle E-Eval-Ctxt and E-Put-Err, or do we need to look at all the cases?

A.5. Proof of Lemma 2.5

Proof. By induction on the derivation of $\sigma \hookrightarrow \sigma_a$, by cases on the last rule in the derivation.

- E-Eval-Ctxt: TODO: Figure out what to do here. This is the only interesting case. Could we just go case-by-case on evaluation contexts?
- E-Beta: $\sigma = \langle S;\ (\lambda x.\, e)\ v \rangle$, and $\sigma_a = \langle S;\ e[x := v] \rangle$.

  Given:

  - $\langle S;\ (\lambda x.\, e)\ v \rangle \hookrightarrow \langle S;\ e[x := v] \rangle$, and
  - $\langle S;\ (\lambda x.\, e)\ v \rangle \hookrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that

  $\langle S;\ e[x := v] \rangle \hookrightarrow^i \sigma_c$ and $\sigma_b \hookrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

  By inspection of the operational semantics, $\sigma_b = \langle S;\ e[x := v] \rangle$.

  Choose $\sigma_c = \langle S;\ e[x := v] \rangle$, $i = 0$ and $j = 0$.

  Then $\langle S;\ e[x := v] \rangle = \sigma_c$ and $\sigma_b = \sigma_c$, as required.
- E-New: $\sigma = \langle S;\ \texttt{new} \rangle$, and $\sigma_a = \langle S[l \mapsto \bot];\ l \rangle$.

  Given:

  - $\langle S;\ \texttt{new} \rangle \hookrightarrow \langle S[l \mapsto \bot];\ l \rangle$, and

  - $\langle S;\, \texttt{new}\rangle \hookrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that

  $\langle S[l \mapsto \bot];\, l\rangle \hookrightarrow^i \sigma_c$ and $\sigma_b \hookrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

  By inspection of the operational semantics, $\sigma_b = \langle S[l' \mapsto \bot];\, l'\rangle$.

  From the side condition of E-New, $l \notin S$.

  Therefore, in $\langle S[l' \mapsto \bot];\, l'\rangle$, we can α-rename l' to l, resulting in $\langle S[l \mapsto \bot];\, l\rangle$.

  Choose $\sigma_c = \langle S[l \mapsto \bot];\, l\rangle$, $i = 0$ and $j = 0$.

  Then $\langle S;\, e[x := v]\rangle = \sigma_c$ and $\sigma_b = \sigma_c$, as required.

- E-Put: $\sigma = \langle S;\, \texttt{put}\ l\ d_2\rangle$, and $\sigma_a = \langle S[l \mapsto d_2];\, \texttt{()}\rangle$.

  Given:

  - $\langle S;\, \texttt{put}\ l\ d_2\rangle \hookrightarrow \langle S[l \mapsto d_2];\, \texttt{()}\rangle$, and
  - $\langle S;\, \texttt{put}\ l\ d_2\rangle \hookrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that

  $\langle S[l \mapsto d_2];\, \texttt{()}\rangle \hookrightarrow^i \sigma_c$ and $\sigma_b \hookrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

  By inspection of the operational semantics, $\sigma_b = \langle S[l \mapsto d_2];\, \texttt{()}\rangle$.

  Choose $\sigma_c = \langle S[l \mapsto d_2];\, \texttt{()}\rangle$, $i = 0$ and $j = 0$.

  Then $\langle S[l \mapsto d_2];\, \texttt{()}\rangle = \sigma_c$ and $\sigma_b = \sigma_c$, as required.

- E-Put-Err: $\sigma = \langle S;\, \texttt{put}\ l\ d_2\rangle$, and $\sigma_a = \textbf{error}$.

  Given:

  - $\langle S;\, \texttt{put}\ l\ d_2\rangle \hookrightarrow \textbf{error}$, and
  - $\langle S;\, \texttt{put}\ l\ d_2\rangle \hookrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that

  error $\hookrightarrow^i \sigma_c$ and $\sigma_b \hookrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

  By inspection of the operational semantics, $\sigma_b = \textbf{error}$.

  Choose $\sigma_c = \textbf{error}$, $i = 0$ and $j = 0$.

  Then **error** $= \sigma_c$ and $\sigma_b = \sigma_c$, as required.

- E-Get: $\sigma = \langle S;\, \texttt{get}\ l\ T\rangle$, and $\sigma_a = \langle S;\, d_2\rangle$.

  Given:

  - $\langle S;\, \texttt{get}\ l\ T\rangle \hookrightarrow \langle S;\, d_2\rangle$, and

- $\langle S;\, \texttt{get}\, l\, T\rangle \hookrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that

  $\langle S;\, d_2\rangle \hookrightarrow^i \sigma_c$ and $\sigma_b \hookrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

  By inspection of the operational semantics, $\sigma_b = \langle S;\, d_2\rangle$.

  Choose $\sigma_c = \langle S;\, d_2\rangle$, $i = 0$ and $j = 0$.

  Then $\langle S;\, d_2\rangle = \sigma_c$ and $\sigma_b = \sigma_c$, as required.

□

A.6. Proof of Lemma 2.6

Proof. We proceed by induction on m. In the base case of $m = 1$, the result is immediate from Lemma 2.5.

For the induction step, suppose $\sigma \hookrightarrow^m \sigma'' \hookrightarrow \sigma'''$ and suppose the lemma holds for m.

We show that it holds for $m + 1$, as follows.

We are required to show that there exist σ_c, i, j such that $\sigma' \hookrightarrow^i \sigma_c$ and $\sigma''' \hookrightarrow^j \sigma_c$ and $i \leq m + 1$ and $j \leq 1$.

From the induction hypothesis, we have that there exist σ'_c, i', j' such that $\sigma' \hookrightarrow^{i'} \sigma'_c$ and $\sigma'' \hookrightarrow^{j'} \sigma'_c$ and $i' \leq m$ and $j' \leq 1$.

We proceed by cases on j':

- If $j' = 0$, then $\sigma'' = \sigma'_c$. We can then choose $\sigma_c = \sigma'''$ and $i = i' + 1$ and $j = 0$.
- If $j' = 1$: From $\sigma'' \hookrightarrow \sigma'''$ and $\sigma'' \hookrightarrow^{j'} \sigma'_c$ and Lemma 2.5, we have that there exist σ''_c and i'' and j'' such that $\sigma'_c \hookrightarrow^{i''} \sigma''_c$ and $\sigma''' \hookrightarrow^{j''} \sigma''_c$ and $i'' \leq 1$ and $j'' \leq 1$.

  So we also have $\sigma' \hookrightarrow^{i'} \sigma'_c \hookrightarrow^{i''} \sigma''_c$. In summary, we pick $\sigma_c = \sigma''_c$ and $i = i' + i''$ and $j = j''$, which is sufficient because $i = i' + i'' \leq m + 1$ and $j = j'' \leq 1$.

□

A.7. Proof of Lemma 2.7

Proof. We proceed by induction on n. In the base case of $n = 1$, the result is immediate from Lemma 2.6.

For the induction step, suppose $\sigma \hookrightarrow^n \sigma' \hookrightarrow \sigma'''$ and suppose the lemma holds for n.

We show that it holds for $n + 1$, as follows.

We are required to show that there exist σ_c, i, j such that $\sigma''' \hookrightarrow^i \sigma_c$ and $\sigma'' \hookrightarrow^j \sigma_c$ and $i \leq m$ and $j \leq n + 1$.

From the induction hypothesis, we have that there exist σ'_c, i', j' such that $\sigma' \hookrightarrow^{i'} \sigma'_c$ and $\sigma'' \hookrightarrow^{j'} \sigma'_c$ and $i' \leq m$ and $j' \leq n$.

We proceed by cases on i':

- If $i' = 0$, then $\sigma' = \sigma'_c$. We can then choose $\sigma_c = \sigma'''$ and $i = 0$ and $j = j' + 1$.
- If $i' \geq 1$:

  From $\sigma' \hookrightarrow \sigma'''$ and $\sigma' \hookrightarrow^{i'} \sigma'_c$ and Lemma 2.6, we have that there exist σ''_c and i'' and j'' such that $\sigma''' \hookrightarrow^{i''} \sigma''_c$ and $\sigma'_c \hookrightarrow^{j''} \sigma''_c$ and $i'' \leq i'$ and $j'' \leq 1$. So we also have $\sigma'' \hookrightarrow^{j'} \sigma'_c \hookrightarrow^{j''} \sigma''_c$. In summary, we pick $\sigma_c = \sigma''_c$ and $i = i''$ and $j = j' + j''$, which is sufficient because $i = i'' \leq i' \leq m$ and $j = j' + j'' \leq n + 1$.

□

A.8. Proof of Lemma 3.2

Proof.

(1) $\sqsubseteq_p$ is a partial order over D_p.

   To show this, we need to show that $\sqsubseteq_p$ is reflexive, transitive, and antisymmetric.

   (a) $\sqsubseteq_p$ is reflexive.

      Suppose $v \in D_p$. Then, by Lemma 3.1, either $v = (d, \text{false})$ with $d \in D$, or $v = (x, \text{true})$ with $x \in X$, where $X = D - \{\top\}$.

      - Suppose $v = (d, \text{false})$:

By the reflexivity of $\sqsubseteq$, we know $d \sqsubseteq d$.

By the definition of $\sqsubseteq_p$, we know $(d, \text{false}) \sqsubseteq_p (d, \text{false})$.

- Suppose $v = (x, \text{true})$:

  By the reflexivity of equality, $x = x$.

  By the definition of $\sqsubseteq_p$, we know $(x, \text{true}) \sqsubseteq_p (x, \text{true})$.

(b) $\sqsubseteq_p$ is transitive.

Suppose $v_1 \sqsubseteq_p v_2$ and $v_2 \sqsubseteq_p v_3$. We want to show that $v_1 \sqsubseteq_p v_3$. We proceed by case analysis on v_1, v_2, and v_3.

- Case $v_1 = (d_1, \text{false})$ and $v_2 = (d_2, \text{false})$ and $v_3 = (d_3, \text{false})$:

  By inversion on $\sqsubseteq_p$, it follows that $d_1 \sqsubseteq d_2$.

  By inversion on $\sqsubseteq_p$, it follows that $d_2 \sqsubseteq d_3$.

  By the transitivity of $\sqsubseteq$, we know $d_1 \sqsubseteq d_3$.

  By the definition of $\sqsubseteq_p$, it follows that $(d_1, \text{false}) \sqsubseteq_p (d_3, \text{false})$.

  Hence $v_1 \sqsubseteq_p v_3$.

- Case $v_1 = (d_1, \text{false})$ and $v_2 = (d_2, \text{false})$ and $v_3 = (x_3, \text{true})$:

  By inversion on $\sqsubseteq_p$, it follows that $d_1 \sqsubseteq d_2$.

  By inversion on $\sqsubseteq_p$, it follows that $d_2 \sqsubseteq x_3$.

  By the transitivity of $\sqsubseteq$, we know $d_1 \sqsubseteq x_3$.

  By the definition of $\sqsubseteq_p$, it follows that $(d_1, \text{false}) \sqsubseteq_p (x_3, \text{true})$.

  Hence $v_1 \sqsubseteq_p v_3$.

- Case $v_1 = (d_1, \text{false})$ and $v_2 = (x_2, \text{true})$ and $v_3 = (d_3, \text{false})$:

  By inversion on $\sqsubseteq_p$, it follows that $d_1 \sqsubseteq x_2$.

  By inversion on $\sqsubseteq_p$, it follows that $d_3 = \top$.

  Since $\top$ is the maximal element of D, we know $d_1 \sqsubseteq \top \equiv d_3$.

  By the definition of $\sqsubseteq_p$, it follows that $(d_1, \text{false}) \sqsubseteq_p (d_3, \text{false})$.

  Hence $v_1 \sqsubseteq_p v_3$.

- Case $v_1 = (d_1, \text{false})$ and $v_2 = (x_2, \text{true})$ and $v_3 = (x_3, \text{true})$:

  By inversion on $\sqsubseteq_p$, it follows that $d_1 \sqsubseteq x_2$.

  By inversion on $\sqsubseteq_p$, it follows that $x_2 = x_3$.

Hence $d_1 \sqsubseteq x_3$.

By the definition of $\sqsubseteq_p$, it follows that $(d_1, \text{false}) \sqsubseteq_p (x_3, \text{true})$.

Hence $v_1 \sqsubseteq_p v_3$.

- Case $v_1 = (x_1, \text{true})$ and $v_2 = (d_2, \text{false})$ and $v_3 = (d_3, \text{false})$:

  By inversion on $\sqsubseteq_p$, it follows that $d_2 = \top$.

  By inversion on $\sqsubseteq_p$, it follows that $d_2 \sqsubseteq d_3$.

  Since $\top$ is maximal, it follows that $d_3 = \top$.

  By the definition of $\sqsubseteq_p$, it follows that $(x_1, \text{true}) \sqsubseteq_p (d_3, \text{false})$.

  Hence $v_1 \sqsubseteq_p v_3$.

- Case $v_1 = (x_1, \text{true})$ and $v_2 = (d_2, \text{false})$ and $v_3 = (x_3, \text{true})$:

  By inversion on $\sqsubseteq_p$, it follows that $d_2 = \top$.

  By inversion on $\sqsubseteq_p$, it follows that $d_2 \sqsubseteq x_3$.

  Since $\top$ is maximal, it follows that $x_3 = \top$.

  But since $x_3 \in X \subseteq D / \{\top\}$, we know $x_3 \neq \top$.

  This is a contradiction.

  Hence $v_1 \sqsubseteq_p v_3$.

- Case $v_1 = (x_1, \text{true})$ and $v_2 = (x_2, \text{true})$ and $v_3 = (d_3, \text{false})$:

  By inversion on $\sqsubseteq_p$, it follows that $x_1 = x_2$.

  By inversion on $\sqsubseteq_p$, it follows that $d_3 = \top$.

  By the definition of $\sqsubseteq_p$, it follows that $(x_1, \text{true}) \sqsubseteq_p (d_3, \text{false})$.

  Hence $v_1 \sqsubseteq_p v_3$.

- Case $v_1 = (x_1, \text{true})$ and $v_2 = (x_2, \text{true})$ and $v_3 = (x_3, \text{true})$:

  By inversion on $\sqsubseteq_p$, it follows that $x_1 = x_2$.

  By inversion on $\sqsubseteq_p$, it follows that $x_2 = x_3$.

  By transitivity of $=$, $x_1 = x_3$.

  By the definition of $\sqsubseteq_p$, it follows that $(x_1, \text{true}) \sqsubseteq_p (x_3, \text{true})$.

  Hence $v_1 \sqsubseteq_p v_3$.

(c) $\sqsubseteq_p$ is antisymmetric.

Suppose $v_1 \sqsubseteq_p v_2$ and $v_2 \sqsubseteq_p v_1$. Now, we proceed by cases on v_1 and v_2.

- Case $v_1 = (d_1, \text{false})$ and $v_2 = (d_2, \text{false})$:

  By inversion on $v_1 \sqsubseteq_p v_2$, we know that $d_1 \sqsubseteq d_2$.

  By inversion on $v_2 \sqsubseteq_p v_1$, we know that $d_2 \sqsubseteq d_1$.

  By the antisymmetry of $\leq$, we know $d_1 = d_2$.

  Hence $v_1 = v_2$.

- Case $v_1 = (d_1, \text{false})$ and $v_2 = (x_2, \text{true})$:

  By inversion on $v_1 \sqsubseteq_p v_2$, we know that $d_1 \sqsubseteq x_2$.

  By inversion on $v_2 \sqsubseteq_p v_1$, we know that $d_1 = \top$.

  Since $\top$ is maximal in D, we know $x_2 = \top$.

  But since $x_2 \in X \subseteq D / \{\top\}$, we know $x_2 \neq \top$.

  This is a contradiction.

  Hence $v_1 = v_2$.

- Case $v_1 = (x_1, \text{true})$ and $v_2 = (d_2, \text{false})$:

  Similar to the previous case.

- Case $v_1 = (x_1, \text{true})$ and $v_2 = (x_2, \text{true})$:

  By inversion on $v_1 \sqsubseteq_p v_2$, we know that $x_1 = x_2$.

  Hence $v_1 = v_2$.

(2) Every nonempty finite subset of D_p has a least upper bound.

To show this, it is sufficient to show that every two elements of D_p have a least upper bound, since a binary least upper bound operation can be repeatedly applied to compute the least upper bound of any finite set. We will show that every two elements of D_p have a least upper bound by showing that the $\sqcup_p$ operation defined by Definition 3.2 computes their least upper bound.

It suffices to show the following two properties:

(a) For all $v_1, v_2, v \in D_p$, if $v_1 \sqsubseteq_p v$ and $v_2 \sqsubseteq_p v$, then $(v_1 \sqcup_p v_2) \sqsubseteq_p v$.

(b) For all $v_1, v_2 \in D_p$, $v_1 \sqsubseteq_p (v_1 \sqcup_p v_2)$ and $v_2 \sqsubseteq_p (v_1 \sqcup_p v_2)$.

(a) For all $v_1, v_2, v \in D_p$, if $v_1 \sqsubseteq_p v$ and $v_2 \sqsubseteq_p v$, then $v_1 \sqcup_p v_2 \sqsubseteq_p v$.

Assume $v_1, v_2, v \in D_p$, and $v_1 \sqsubseteq_p v$ and $v_2 \sqsubseteq_p v$. Now we do a case analysis on v_1 and v_2.

- Case $v_1 = (d_1, \text{false})$ and $v_2 = (d_2, \text{false})$.

  Now case on v:

- Case $v = (d, \text{false})$:

  By the definition of $\sqcup_p$, $(d_1, \text{false}) \sqcup_p (d_2, \text{false}) = (d_1 \sqcup d_2, \text{false})$.

  By inversion on $(d_1, \text{false}) \sqsubseteq_p (d, \text{false})$, $d_1 \sqsubseteq l$.

  By inversion on $(d_2, \text{false}) \sqsubseteq_p (d, \text{false})$, $d_2 \sqsubseteq l$.

  Hence l is an upper bound for d_1 and d_2.

  Hence $d_1 \sqcup d_2 \sqsubseteq l$.

  Hence $(d_1 \sqcup d_2, \text{false}) \sqsubseteq_p (d, \text{false})$.

  Hence $v_1 \sqcup_p v_2 \sqsubseteq_p v$.

- Case $v = (x, \text{true})$:

  By the definition of $\sqcup_p$, $(d_1, \text{false}) \sqcup_p (d_2, \text{false}) = (d_1 \sqcup d_2, \text{false})$.

  By inversion on $(d_1, \text{false}) \sqsubseteq_p (x, \text{true})$, $d_1 \sqsubseteq x$.

  By inversion on $(d_2, \text{false}) \sqsubseteq_p (x, \text{true})$, $d_2 \sqsubseteq x$.

  Hence x is an upper bound for d_1 and d_2.

  Hence $d_1 \sqcup d_2 \sqsubseteq x$.

  Hence $(d_1 \sqcup d_2, \text{false}) \sqsubseteq_p (x, \text{true})$.

  Hence $v_1 \sqcup_p v_2 \sqsubseteq_p v$.

- Case $v_1 = (x_1, \text{true})$ and $v_2 = (x_2, \text{true})$:

  Now case on v:

  - Case $v = (d, \text{false})$:

    By inversion on $(x_1, \text{true}) \sqsubseteq_p (d, \text{false})$, we know $l = \top$.

    By inversion on $(x_2, \text{true}) \sqsubseteq_p (d, \text{false})$, we know $l = \top$.

    Now consider whether $x_1 = x_2$ or not. If it does, then by the definition of $\sqcup_p$, $(x_1, \text{true}) \sqcup_p (x_2, \text{true}) = (x_1, \text{true})$.

    By definition of $\sqsubseteq_p$, we have $(x_1, \text{true}) \sqsubseteq_p (\top, \text{false})$. So $v_1 \sqcup_p v_2 \sqsubseteq_p v$.

    If it does not, then $v_1 \sqcup_p v_2 = (\top, \text{false})$.

    By the definition of $\sqsubseteq_p$, we have $(\top, \text{false}) \sqsubseteq_p (\top, \text{false})$. So $v_1 \sqcup_p v_2 \sqsubseteq_p v$.

  - Case $v = (x, \text{true})$:

    By inversion on $(x_1, \text{true}) \sqsubseteq_p (x, \text{true})$, we know $x = x_1$.

    By inversion on $(x_2, \text{true}) \sqsubseteq_p (x, \text{true})$, we know $x = x_2$.

Hence $x_1 = x_2$.

By the definition of $\sqcup_p$, $(x_1, \text{true}) \sqcup_p (x_2, \text{true}) = (x_1, \text{true})$.

Hence $v_1 \sqcup_p v_2 \sqsubseteq_p v$.

- Case $v_1 = (x_1, \text{true})$ and $v_2 = (d_2, \text{false})$:

  Now case on v:

  – Case $v = (d, \text{false})$:

  Now consider whether $d_2 \sqsubseteq x_1$.

  If it is, then $(x_1, \text{true}) \sqcup_p (d_2, \text{false}) = (x_1, \text{true}) = v_1$.

  Hence $v_1 \sqcup_p v_2 \sqsubseteq_p v$.

  Otherwise, $(x_1, \text{true}) \sqcup_p (d_2, \text{false}) = (\top, \text{false})$.

  By inversion on $(x_1, \text{true}) \sqsubseteq_p (d, \text{false})$, we know $l = \top$.

  By reflexivity, $(\top, \text{false}) \sqsubseteq_p (\top, \text{false})$.

  Hence $v_1 \sqcup_p v_2 \sqsubseteq_p v$.

  – Case $v = (x, \text{true})$:

  By inversion on $(x_1, \text{true}) \sqsubseteq_p (x, \text{true})$, we know that $x_1 = x$.

  By inversion on $(d_2, \text{false}) \sqsubseteq_p (x, \text{true})$, we know that $d_2 \sqsubseteq x$.

  By transitivity, $d_2 \sqsubseteq x_1$.

  By the definition of $\sqcup_p$, it follows that $(x_1, \text{true}) \sqcup_p (d_2, \text{false}) = (x_1, \text{true})$.

  By defininition of $\sqsubseteq_p$, $(x_1, \text{true}) \sqsubseteq_p (x_1, \text{true})$.

  Hence $v_1 \sqcup_p v_2 \sqsubseteq_p v$.

- Case $v_1 = (d_1, \text{false})$ and $v_2 = (x_2, \text{true})$:

  Symmetric with the previous case.

(b) For all $v_1, v_2 \in D_p$, $v_1 \sqsubseteq_p v_1 \sqcup_p v_2$ and $v_2 \sqsubseteq_p v_1 \sqcup_p v_2$.

Assume $v_1, v_2 \in D_p$, and proceed by case analysis.

- Case $v_1 = (d_1, \text{false})$ and $v_2 = (d_2, \text{false})$:

  Since $\sqcup$ is a join operator, we know $d_1 \sqsubseteq d_1 \sqcup d_2$.

  By the definition of $\sqsubseteq_p$, $(d_1, \text{false}) \sqsubseteq (d_1 \sqcup d_2, \text{false})$.

  By the definition of $\sqcup_p$, $v_1 \sqcup_p v_2 = (d_1 \sqcup d_2, \text{false})$.

Hence $v_1 \sqsubseteq_p v_1 \sqcup_p v_2$.

Since $\sqcup$ is a join operator, we know $d_1 \sqsubseteq d_1 \sqcup d_2$.

By the definition of $\sqsubseteq_p$, $(d_2, \text{false}) \sqsubseteq (d_1 \sqcup d_2, \text{false})$.

By the definition of $\sqcup_p$, $v_1 \sqcup_p v_2 = (d_1 \sqcup d_2, \text{false})$.

Hence $v_2 \sqsubseteq_p v_1 \sqcup_p v_2$.

Therefore $v_1 \sqsubseteq_p v_1 \sqcup v_2$ and $v_2 \sqsubseteq_p v_1 \sqcup v_2$.

- Case $v_1 = (d_1, \text{false})$ and $v_2 = (x_2, \text{true})$:

  Consider whether $d_1 \sqsubseteq x_2$.

  - Case $d_1 \sqsubseteq x_2$:

    By the definition of $\sqcup_p$, we know $(d_1, \text{false}) \sqcup_p (x_2, \text{true}) = (x_2, \text{true})$.

    By the definition of $\sqcup_p$, we know $(d_1, \text{false}) \sqsubseteq_p (x_2, \text{true})$.

    Hence $v_1 \sqsubseteq_p v_1 \sqcup_p v_2$.

    By reflexivity, $(x_2, \text{true}) \sqsubseteq_p (x_2, \text{true})$.

    Hence $v_2 \sqsubseteq_p v_1 \sqcup_p v_2$.

    Therefore $v_1 \sqsubseteq_p v_1 \sqcup v_2$ and $v_2 \sqsubseteq_p v_1 \sqcup v_2$.

  - Case $d_1 \not\sqsubseteq x_2$:

    By the definition of $\sqcup_p$, we know $(d_1, \text{false}) \sqcup_p (x_2, \text{true}) = (\top, \text{false})$.

    Since $d_1 \sqsubseteq \top$, by the definition of $\sqsubseteq_p$ we know $(d_1, \text{false}) \sqsubseteq (\top, \text{false})$.

    Hence $v_1 \sqsubseteq_p v_1 \sqcup_p v_2$.

    By the definition of $\sqsubseteq_p$, we know $(x_2, \text{true}) \sqsubseteq (\top, \text{false})$.

    Hence $v_2 \sqsubseteq_p v_1 \sqcup_p v_2$.

    Therefore $v_1 \sqsubseteq_p v_1 \sqcup v_2$ and $v_2 \sqsubseteq_p v_1 \sqcup v_2$.

- Case $v_1 = (x_1, \text{true})$ and $v_2 = (d_2, \text{false})$:

  Symmetric with the previous case.

- Case $v_1 = (x_1, \text{true})$ and $v_2 = (x_2, \text{true})$:

  Consider whether x_1 equals x_2.

  - Case $x_1 = x_2$:

By the definition $\sqcup_p$, $(x_1, \text{true}) \sqcup_p (x_2, \text{true}) = (x_1, \text{true})$.

By reflexivity, $(x_1, \text{true}) \sqsubseteq_p (x_1, \text{true})$.

Hence $v_1 \sqsubseteq_p v_1 \sqcup_p v_2$.

By reflexivity, $(x_2, \text{true}) \sqsubseteq_p (x_1, \text{true})$.

Hence $v_2 \sqsubseteq_p v_1 \sqcup_p v_2$.

Therefore $v_1 \sqsubseteq_p v_1 \sqcup v_2$ and $v_2 \sqsubseteq_p v_1 \sqcup v_2$.

– Case $x_1 \neq x_2$:

By the definition $\sqcup_p$, $(x_1, \text{true}) \sqcup_p (x_2, \text{true}) = (\top, \text{false})$.

By the definition of $\sqsubseteq_p$, $(x_1, \text{true}) \sqsubseteq_p (\top, \text{false})$.

Hence $v_1 \sqsubseteq_p v_1 \sqcup_p v_2$.

By the definition of $\sqsubseteq_p$, $(x_2, \text{true}) \sqsubseteq_p (\top, \text{false})$.

Hence $v_2 \sqsubseteq_p v_1 \sqcup_p v_2$.

Therefore $v_1 \sqsubseteq_p v_1 \sqcup v_2$ and $v_2 \sqsubseteq_p v_1 \sqcup v_2$.

(3) $\perp_p$ is the least element of D_p.

$\perp_p$ is defined to be $(\perp, \text{false})$. In order to be the least element of D_p, it must be less than or equal to every element of D_p. By Lemma 3.1, the elements of D_p partition into (d, false) for all $d \in D$, and (x, true) for all $x \in X$, where $X = D - \{\top\}$.

We consider both cases:

- (d, false) for all $d \in D$:

  By the definition of $\sqsubseteq_p$, $(\perp, \text{false}) \sqsubseteq_p (d, \text{false})$ iff $\perp \sqsubseteq d$.

  Since $\perp$ is the least element of D, $\perp \sqsubseteq d$.

  Therefore $\perp_p = (\perp, \text{false}) \sqsubseteq_p (d, \text{false})$.

- (x, true) for all $x \in X$:

  By the definition of $\sqsubseteq_p$, $(\perp, \text{false}) \sqsubseteq_p (x, \text{true})$ iff $\perp \sqsubseteq x$.

  Since $\perp$ is the least element of D, $\perp \sqsubseteq x$.

  Therefore $\perp_p = (\perp, \text{false}) \sqsubseteq_p (x, \text{true})$.

Therefore $\perp_p$ is less than or equal to all elements of D_p.

(4) $\top_p$ is the greatest element of D_p.

$\top_p$ is defined to be $(\top, \text{false})$. In order to be the greatest element of D_p, every element of D_p must be less than or equal to it. By Lemma 3.1, the elements of D_p partition into (d, false) for all $d \in D$, and (x, true) for all $x \in X$, where $X = D - \{\top\}$.

We consider both cases:

- (d, false) for all $d \in D$:

  By the definition of $\sqsubseteq_p$, $(d, \text{false}) \sqsubseteq_p (\top, \text{false})$ iff $d \sqsubseteq \top$.

  Since $\top$ is the greatest element of D, $d \sqsubseteq \top$.

  Therefore $(d, \text{false}) \sqsubseteq_p (\top, \text{false}) = \top_p$.

- (x, true) for all $x \in X$:

  By the definition of $\sqsubseteq_p$, $(x, \text{true}) \sqsubseteq_p (\top, \text{false})$ iff $\top \sqsubseteq \top$.

  Therefore $(x, \text{true}) \sqsubseteq_p (\top, \text{false}) = \top_p$.

Therefore all elements of D_p are less than or equal to $\top_p$.

□

A.9. Proof of Lemma 3.3

Proof.

- Case E-Eval-Ctxt:

  Given: $\langle S;\ E[e]\rangle \hookrightarrow \langle S';\ E[e']\rangle$.

  To show: $S \sqsubseteq_S S'$.

  From the premise of E-Eval-Ctxt, $\langle S;\ e\rangle \hookrightarrow \langle S';\ e'\rangle$.

  Hence by IH, $S \sqsubseteq_S S'$, as we were required to show.

- Case E-Beta:

  Immediate by the definition of $\sqsubseteq_S$, since S does not change.

- Case E-New:

  Given: $\langle S;\ \texttt{new}\rangle \hookrightarrow \langle S[l \mapsto (\bot, \text{false})];\ l\rangle$.

  To show: $S \sqsubseteq_S S[l \mapsto (\bot, \text{false})]$.

  By Definition 3.4, we have to show that $\mathit{dom}(S) \subseteq \mathit{dom}(S[l \mapsto (\bot, \text{false})])$ and that for all $l' \in \mathit{dom}(S)$,

  $S(l') \sqsubseteq_p (S[l \mapsto (\bot, \text{false})])(l')$.

By the definition of store update, $S[l \mapsto (d_1, \text{true})]$ can only either update an existing binding in S or extend S with a new binding.

Hence *dom*$(S) \subseteq$ *dom*$(S[l \mapsto (\bot, \text{false})])$.

From the side condition of E-New, $l \notin$ *dom*(S).

Hence $S[l \mapsto (\bot, \text{false})]$ adds a new binding for l in S.

Hence $S[l \mapsto (d_1, \text{true})]$ does not update any existing bindings in S.

Hence, for all $l' \in$ *dom*(S), $S(l') \sqsubseteq_p (S[l \mapsto (d_1, \text{true})])(l')$.

Therefore $S \sqsubseteq_S S[l \mapsto (\bot, \text{false})]$, as required.

- Case E-Put:

  Given: $\langle S;\ \texttt{put}\ l\ d_2 \rangle \longleftrightarrow \langle S[l \mapsto p_2];\ \texttt{()} \rangle$.

  To show: $S \sqsubseteq_S S[l \mapsto p_2]$.

  By Definition 3.4, we have to show that *dom*$(S) \subseteq$ *dom*$(S[l \mapsto p_2])$ and that for all $l' \in$ *dom*(S), $S(l') \sqsubseteq_p (S[l \mapsto p_2])(l')$.

  By the definition of store update, $S[l \mapsto p_2]$ can only either update an existing binding in S or extend S with a new binding.

  Hence *dom*$(S) \subseteq$ *dom*$(S[l \mapsto p_2])$.

  From the premises of E-Put, $S(l) = p_1$. Therefore $l \in$ *dom*(S).

  Hence $S[l \mapsto p_2]$ updates the existing binding for l in S from p_1 to p_2.

  From the premises of E-Put, $p_2 = p_1 \sqcup_p (d_2, \text{false})$.

  Hence, by the definition of $\sqcup_p$, $p_1 \sqsubseteq_p p_2$.

  $S[l \mapsto p_2]$ does not update any other bindings in S, hence, for all $l' \in$ *dom*(S), $S(l') \sqsubseteq_p (S[l \mapsto p_2])(l')$.

  Hence $S \sqsubseteq_S S[l \mapsto p_2]$, as required.

- Case E-Put-Err:

  Given: $\langle S;\ \texttt{put}\ l\ d_2 \rangle \longleftrightarrow$ **error**.

  By the definition of **error**, **error** $= \langle \top_S;\ e \rangle$ for any e.

  To show: $S \sqsubseteq_S \top_S$.

  Immediate by the definition of $\sqsubseteq_S$.

- Case E-Get:

Immediate by the definition of $\sqsubseteq_S$, since S does not change.

- Case E-Freeze-Init:

  Immediate by the definition of $\sqsubseteq_S$, since S does not change.

- Case E-Spawn-Handler:

  Immediate by the definition of $\sqsubseteq_S$, since S does not change.

- Case E-Freeze-Final:

  Given: $\langle S; \texttt{freeze}\, l \,\texttt{after}\, Q \,\texttt{with}\, v, \{v \dots\}, H \rangle \hookrightarrow \langle S[l \mapsto (d_1, \text{true})]; \, d_1 \rangle$.

  To show: $S \sqsubseteq_S S[l \mapsto (d_1, \text{true})]$.

  By Definition 3.4, we have to show that $\mathit{dom}(S) \subseteq \mathit{dom}(S[l \mapsto (d_1, \text{true})])$ and that for all $l' \in \mathit{dom}(S)$,

  $S(l') \sqsubseteq_p (S[l \mapsto (d_1, \text{true})])(l')$.

  LK: We could spell this out in even more excruciating detail, but I think it's obvious enough.

  By the definition of store update, $S[l \mapsto (d_1, \text{true})]$ can only either update an existing binding in S or extend S with a new binding.

  Hence $\mathit{dom}(S) \subseteq \mathit{dom}(S[l \mapsto (d_1, \text{true})])$.

  From the premises of E-Freeze-Final, $S(l) = (d_1, \mathit{frz}_1)$. Therefore $l \in \mathit{dom}(S)$.

  Hence $S[l \mapsto (d_1, \text{true})]$ updates the existing binding for l in S from (d_1, frz_1) to (d_1, true).

  By the definition of $\sqsubseteq_p$, $(d_1, \mathit{frz}_1) \sqsubseteq_p (d_1, \text{true})$.

  $S[l \mapsto (d_1, \text{true})]$ does not update any other bindings in S, hence, for all $l' \in \mathit{dom}(S)$,

  $S(l') \sqsubseteq_p (S[l \mapsto (d_1, \text{true})])(l')$.

  Hence $S \sqsubseteq_S S[l \mapsto (d_1, \text{true})]$, as required.

- Case E-Freeze-Simple:

  Given: $\langle S; \texttt{freeze}\, l \rangle \hookrightarrow \langle S[l \mapsto (d_1, \text{true})]; \, d_1 \rangle$.

  To show: $S \sqsubseteq_S S[l \mapsto (d_1, \text{true})]$.

  Similar to the previous case.

□

A.10. Proof of Lemma 3.4

Proof. Consider arbitrary S'' such that S'' is non-conflicting with $\langle S;\, e\rangle \hookrightarrow \langle S';\, e'\rangle$ and $S' \sqcup_S S'' =_{\mathit{frz}} S$ and $S' \sqcup_S S'' \neq \top_S$.

To show: $\langle S \sqcup_S S'';\, e\rangle \hookrightarrow \langle S' \sqcup_S S'';\, e'\rangle$.

The proof is by induction on the derivation of $\langle S;\, e\rangle \hookrightarrow \langle S';\, e'\rangle$, by cases on the last rule in the derivation. In every case we may assume that $\langle S';\, e'\rangle \neq$ **error**. Since $\langle S';\, e'\rangle \neq$ **error**, we do not need to consider the E-Put-Err rule.

The assumption that $S' \sqcup_S S'' =_{\mathit{frz}} S$ is only needed in the E-Freeze-Final and E-Freeze-Simple cases.

- Case E-Eval-Ctxt:

  Given: $\langle S;\, E[e]\rangle \hookrightarrow \langle S';\, E[e']\rangle$.

  To show: $\langle S \sqcup_S S'';\, E[e]\rangle \hookrightarrow \langle S' \sqcup_S S'';\, E[e']\rangle$.

  From the premise of E-Eval-Ctxt, we have that $\langle S;\, e\rangle \hookrightarrow \langle S';\, e'\rangle$.

  Therefore, by IH, we have that $\langle S \sqcup_S S'';\, e\rangle \hookrightarrow \langle S' \sqcup_S S'';\, e'\rangle$.

  Therefore, by E-Eval-Ctxt, we have that $\langle S \sqcup_S S'';\, E[e]\rangle \hookrightarrow \langle S' \sqcup_S S'';\, E[e']\rangle$, as we were required to show.

- Case E-Beta:

  Given: $\langle S;\, (\lambda x.\, e)\, v\rangle \hookrightarrow \langle S;\, e[x := v]\rangle$.

  To show: $\langle S \sqcup_S S'';\, (\lambda x.\, e)\, v\rangle \hookrightarrow \langle S \sqcup_S S'';\, e[x := v]\rangle$.

  Immediate by E-Beta.

- Case E-New:

  Given: $\langle S;\, \texttt{new}\rangle \hookrightarrow \langle S[l \mapsto (\bot, \text{false})];\, l\rangle$.

  To show: $\langle S \sqcup_S S'';\, \texttt{new}\rangle \hookrightarrow \langle (S[l \mapsto (\bot, \text{false})]) \sqcup_S S'';\, l\rangle$.

  By E-New, we have that $\langle S \sqcup_S S'';\, \texttt{new}\rangle \hookrightarrow \langle (S \sqcup_S S'')[l' \mapsto (\bot, \text{false})];\, l'\rangle$, where $l' \notin \mathit{dom}(S \sqcup_S S'')$.

  By assumption, S'' is non-conflicting with $\langle S;\, \texttt{new}\rangle \hookrightarrow \langle S[l \mapsto (\bot, \text{false})];\, l\rangle$.

  Therefore $l \notin \mathit{dom}(S'')$.

  From the side condition of E-New, $l \notin \mathit{dom}(S)$.

Therefore $l \notin \mathit{dom}(S \sqcup_S S'')$.

Therefore, in $\langle (S \sqcup_S S'')[l' \mapsto (\bot, \text{false})];\ l' \rangle$, we can α-rename l' to l,

resulting in $\langle (S \sqcup_S S'')[l \mapsto (\bot, \text{false})];\ l \rangle$.

Therefore $\langle S \sqcup_S S'';\ \texttt{new} \rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto (\bot, \text{false})];\ l \rangle$.

Note that:

$$\begin{aligned}
(S \sqcup_S S'')[l \mapsto (\bot, \text{false})] &= S[l \mapsto (\bot, \text{false})] \sqcup_S S''[l \mapsto (\bot, \text{false})] \\
&= S \sqcup_S [l \mapsto (\bot, \text{false})] \sqcup_S S'' \sqcup_S [l \mapsto (\bot, \text{false})] \\
&= S \sqcup_S [l \mapsto (\bot, \text{false})] \sqcup_S S'' \\
&= S[l \mapsto (\bot, \text{false})] \sqcup_S S''.
\end{aligned}$$

Therefore $\langle S \sqcup_S S'';\ \texttt{new} \rangle \hookrightarrow \langle S[l \mapsto (\bot, \text{false})] \sqcup_S S'';\ l \rangle$, as we were required to show.

- Case E-Put:

  LK: The assumption that $S[l \mapsto p_2] \sqcup_S S'' \neq \top_S$ rules out the put-after-freeze possibility.

  Given: $\langle S;\ \texttt{put}\ l\ d_2 \rangle \hookrightarrow \langle S[l \mapsto p_2];\ () \rangle$.

  To show: $\langle S \sqcup_S S'';\ \texttt{put}\ l\ d_2 \rangle \hookrightarrow \langle S[l \mapsto p_2] \sqcup_S S'';\ () \rangle$.

  We will first show that

  $\langle S \sqcup_S S'';\ \texttt{put}\ l\ d_2 \rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto p_2];\ () \rangle$

  and then show why this is sufficient.

  We proceed by cases on l:

  - $l \notin \mathit{dom}(S'')$:

    By assumption, $S[l \mapsto p_2] \sqcup_S S'' \neq \top_S$.

    By Lemma 3.3, $S \sqsubseteq_S S[l \mapsto p_2]$.

    Hence $S \sqcup_S S'' \neq \top_S$.

    Therefore, by Definition 3.5, $(S \sqcup_S S'')(l) = S(l)$.

    From the premises of E-Put, $S(l) = p_1$.

    Hence $(S \sqcup_S S'')(l) = p_1$.

    From the premises of E-Put, $p_2 = p_1 \sqcup_p (d_2, \text{false})$ and $p_2 \neq \top_p$.

    Therefore, by E-Put, we have: $\langle S \sqcup_S S'';\ \texttt{put}\ l\ d_2 \rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto p_2];\ () \rangle$.

  - $l \in \mathit{dom}(S'')$:

By assumption, $S[l \mapsto p_2] \sqcup_S S'' \neq \top_S$.

By Lemma 3.3, $S \sqsubseteq_S S[l \mapsto p_2]$.

Hence $S \sqcup_S S'' \neq \top_S$.

Therefore $(S \sqcup_S S'')(l) = S(l) \sqcup_p S''(l)$.

From the premises of E-Put, $S(l) = p_1$.

Hence $(S \sqcup_S S'')(l) = p'_1$, where $p_1 \sqsubseteq_p p'_1$.

From the premises of E-Put, $p_2 = p_1 \sqcup_p (d_2, \text{false})$.

Let $p'_2 = p'_1 \sqcup_p (d_2, \text{false})$.

Hence $p_2 \sqsubseteq_p p'_2$.

By assumption, $S[l \mapsto p_2] \sqcup_S S'' \neq \top_S$.

Therefore, by Definition 3.5, $p_2 \sqcup_S S''(l) \neq \top_p$.

Note that:

$$\begin{aligned}
\top_p &\neq p_2 \sqcup_S S''(l) \\
&= p_1 \sqcup_p (d_2, \text{false}) \sqcup_p S''(l) \\
&= S(l) \sqcup_p (d_2, \text{false}) \sqcup_p S''(l) \\
&= S(l) \sqcup_p S''(l) \sqcup_p (d_2, \text{false}) \\
&= (S \sqcup_S S'')(l) \sqcup_p (d_2, \text{false}) \\
&= p'_1 \sqcup_p (d_2, \text{false}) \\
&= p'_2.
\end{aligned}$$

Hence $p'_2 \neq \top_p$.

Hence $(S \sqcup_S S'')(l) = p'_1$ and $p'_2 = p'_1 \sqcup_p (d_2, \text{false})$ and $p'_2 \neq \top_p$.

Therefore, by E-Put we have: $\langle S \sqcup_S S''; \ \texttt{put}\ l\ d_2 \rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto p'_2]; \ \texttt{()} \rangle$.

LK: If we really wanted to be pedantic here, we'd actually prove that the stores are equal. I'm assuming that if I can show that $(S \sqcup_S S'')[l \mapsto p'_2]$ and $(S \sqcup_S S'')[l \mapsto p_2]$ bind l to the same value, then it will be obvious that they're equal.

Note that:

$$\begin{aligned}((S \sqcup_S S'')[l \mapsto p'_2])(l) &= (S \sqcup_S S'')(l) \sqcup_p ([l \mapsto p'_2])(l)\\ &= p'_1 \sqcup_p p'_2\\ &= p'_1 \sqcup_p p'_1 \sqcup_p (d_2, \text{false})\\ &= p'_1 \sqcup_p (d_2, \text{false})\end{aligned}$$

and

$$\begin{aligned}((S \sqcup_S S'')[l \mapsto p_2])(l) &= (S \sqcup_S S'')(l) \sqcup_p ([l \mapsto p_2])(l)\\ &= p'_1 \sqcup_p p_2\\ &= p'_1 \sqcup_p p_1 \sqcup_p (d_2, \text{false})\\ &= p'_1 \sqcup_p (d_2, \text{false}) && \text{(since } p_1 \sqsubseteq_p p'_1\text{).}\end{aligned}$$

Therefore $(S \sqcup_S S'')[l \mapsto p'_2] = (S \sqcup_S S'')[l \mapsto p_2]$.

Therefore, $\langle S \sqcup_S S''; \texttt{put}\ l\ d_2\rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto p_2]; \texttt{()}\rangle$.

Note that:

$$\begin{aligned}(S \sqcup_S S'')[l \mapsto p_2] &= S[l \mapsto p_2] \sqcup_S S''[l \mapsto p_2]\\ &= S \sqcup_S [l \mapsto p_2] \sqcup_S S'' \sqcup_S [l \mapsto p_2]\\ &= S \sqcup_S [l \mapsto p_2] \sqcup_S S''\\ &= S[l \mapsto p_2] \sqcup_S S''.\end{aligned}$$

Therefore $\langle S \sqcup_S S''; \texttt{put}\ l\ d_2\rangle \hookrightarrow \langle S[l \mapsto p_2] \sqcup_S S''; \texttt{()}\rangle$, as we were required to show.

- Case E-Get:

  Given: $\langle S; \texttt{get}\ l\ P\rangle \hookrightarrow \langle S; p_2\rangle$.

  To show: $\langle S \sqcup_S S''; \texttt{get}\ l\ P\rangle \hookrightarrow \langle S \sqcup_S S''; p_2\rangle$.

  From the premises of E-Get, $S(l) = p_1$ and *incomp*(P) and $p_2 \in P$ and $p_2 \sqsubseteq_p p_1$.

  By assumption, $S \sqcup_S S'' \neq \top_S$.

  Hence $(S \sqcup_S S'') = p'_1$, where $p_1 \sqsubseteq_p p'_1$.

  By the transitivity of $\sqsubseteq_p$, $p_2 \sqsubseteq_p p'_1$.

  Hence, $S(l) = p'_1$ and *incomp*(P) and $p_2 \in P$ and $p_2 \sqsubseteq_p p'_1$.

Therefore, by E-Get,

$\langle S \sqcup_S S''; \texttt{get}\, l\, P \rangle \hookrightarrow \langle S \sqcup_S S''; p_2 \rangle$,

as we were required to show.

- Case E-Freeze-Init:

  Given: $\langle S; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e \rangle \hookrightarrow$

  $\langle S; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e, \{\}, \{\} \rangle$.

  To show: $\langle S \sqcup_S S''; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e \rangle \hookrightarrow$

  $\langle S \sqcup_S S''; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e, \{\}, \{\} \rangle$.

  Immediate by E-Freeze-Init.

- Case E-Spawn-Handler:

  Given:

  $\langle S; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e, \ldots\}, H \rangle \hookrightarrow$

  $\langle S; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e, \ldots\}, \{d_2\} \cup H \rangle$.

  To show:

  $\langle S \sqcup_S S''; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e, \ldots\}, H \rangle \hookrightarrow$

  $\langle S \sqcup_S S''; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e, \ldots\}, \{d_2\} \cup H \rangle$.

  From the premises of E-Spawn-Handler, $S(l) = (d_1, \mathit{frz}_1)$ and $d_2 \sqsubseteq d_1$ and $d_2 \notin H$ and $d_2 \in Q$.

  By assumption, $S \sqcup_S S'' \neq \top_S$.

  Hence $(S \sqcup_S S'')(l) = (d_1', \mathit{frz}_1')$ where $(d_1, \mathit{frz}_1) \sqsubseteq_p (d_1', \mathit{frz}_1')$.

  By Definition 3.1, $d_1 \sqsubseteq d_1'$.

  By the transitivity of $\sqsubseteq$, $d_2 \sqsubseteq d_1'$.

  Hence $(S \sqcup_S S'')(l) = (d_1', \mathit{frz}_1')$ and $d_2 \sqsubseteq d_1'$ and $d_2 \notin H$ and $d_2 \in Q$.

  Therefore, by E-Spawn-Handler,

  $\langle S \sqcup_S S''; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e, \ldots\}, H \rangle \hookrightarrow$

  $\langle S \sqcup_S S''; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e, \ldots\}, \{d_2\} \cup H \rangle$,

  as we were required to show.

- Case E-Freeze-Final:

  LK: This case wouldn't work but for the $S' \sqcup_S S'' =_{\mathit{frz}} S$ requirement, which makes it a no-op freeze.

Given: $\langle S;\ \texttt{freeze}\,l\,\texttt{after}\,Q\,\texttt{with}\,v, \{v\dots\}, H\rangle \hookrightarrow \langle S[l \mapsto (d_1, \text{true})];\ d_1\rangle$.

To show: $\langle S \sqcup_S S'';\ \texttt{freeze}\,l\,\texttt{after}\,Q\,\texttt{with}\,v, \{v\dots\}, H\rangle \hookrightarrow \langle S[l \mapsto (d_1, \text{true})] \sqcup_S S'';\ d_1\rangle$.

We will first show that

$\langle S \sqcup_S S'';\ \texttt{freeze}\,l\,\texttt{after}\,Q\,\texttt{with}\,v, \{v\dots\}, H\rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \text{true})];\ d_1\rangle$

and then show why this is sufficient.

We proceed by cases on l:

- $l \notin \mathit{dom}(S'')$:

  By assumption, $S[l \mapsto (d_1, \text{true})] \sqcup_S S'' \neq \top_S$.

  By Lemma 3.3, $S \sqsubseteq_S S[l \mapsto (d_1, \text{true})]$.

  Therefore $S \sqcup_S S'' \neq \top_S$.

  Hence, by Definition 3.5, $(S \sqcup_S S'')(l) = S(l)$.

  From the premises of E-Freeze-Final, we have that $S(l) = (d_1, \mathit{frz}_1)$.

  Hence $(S \sqcup_S S'')(l) = (d_1, \mathit{frz}_1)$.

  From the premises of E-Freeze-Final, we have that $\forall d_2 \,.\, (d_2 \sqsubseteq d_1 \wedge d_2 \in Q \Rightarrow d_2 \in H)$.

  Therefore, by E-Freeze-Final, we have that

  $\langle S \sqcup_S S'';\ \texttt{freeze}\,l\,\texttt{after}\,Q\,\texttt{with}\,v, \{v\dots\}, H\rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \text{true})];\ d_1\rangle$.

- $l \in \mathit{dom}(S'')$:

  By assumption, $S[l \mapsto (d_1, \text{true})] \sqcup_S S'' \neq \top_S$.

  By Lemma 3.3, $S \sqsubseteq_S S[l \mapsto (d_1, \text{true})]$.

  Therefore $S \sqcup_S S'' \neq \top_S$.

  Hence, by Definition 3.5, $(S \sqcup_S S'')(l) = S(l) \sqcup_p S''(l)$.

  From the premises of E-Freeze-Final, we have that $S(l) = (d_1, \mathit{frz}_1)$.

  By assumption, $S[l \mapsto (d_1, \text{true})] \sqcup_S S'' =_{\mathit{frz}} S$.

  Therefore $\mathit{frz}_1 = \text{true}$.

  Therefore $S(l) = (d_1, \text{true})$.

  Therefore $(S \sqcup_S S'')(l) = (d_1, \text{true}) \sqcup_p S''(l)$.

  We proceed by cases on $S''(l)$:

  * $S''(l) = (d_3, \text{false})$, where $d_3 \sqsubseteq d_1$:

    By Definition 3.2, $(d_1, \text{true}) \sqcup_p (d_3, \text{false}) = (d_1, \text{true})$.

Therefore $(S \sqcup_S S'')(l) = (d_1, \text{true})$.

From the premises of E-Freeze-Final, we have that $\forall d_2 \,.\, (d_2 \sqsubseteq d_1 \wedge d_2 \in Q \Rightarrow d_2 \in H)$.

Therefore, by E-Freeze-Final, we have that

$\langle S \sqcup_S S'';\ \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, v, \{v \ldots\}, H \rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \text{true})];\ d_1 \rangle$.$\blacksquare$

- $*$ $S''(l) = (d_3, \text{false})$, where $d_3 \not\sqsubseteq d_1$:

By Definition 3.2, $(d_1, \text{true}) \sqcup_p (d_3, \text{false}) = (\top, \text{false})$.

Therefore $S(l) \sqcup_p S''(l) = (\top, \text{false})$.

By Definition 3.1, $(\top, \text{false}) = \top_p$.

Therefore $S(l) \sqcup_p S''(l) = \top_p$.

Therefore, by Definition 3.5, $S \sqcup_S S'' = \top_S$.

This is a contradiction.

Therefore,

$\langle S \sqcup_S S'';\ \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, v, \{v \ldots\}, H \rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \text{true})];\ d_1 \rangle$.$\blacksquare$

- $*$ $S''(l) = (d_3, \text{true})$, where $d_3 = d_1$:

By Definition 3.2, $(d_1, \text{true}) \sqcup_p (d_3, \text{true}) = (d_1, \text{true})$.

Therefore $(S \sqcup_S S'')(l) = (d_1, \text{true})$.

From the premises of E-Freeze-Final, we have that $\forall d_2 \,.\, (d_2 \sqsubseteq d_1 \wedge d_2 \in Q \Rightarrow d_2 \in H)$.

Therefore, by E-Freeze-Final, we have that

$\langle S \sqcup_S S'';\ \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, v, \{v \ldots\}, H \rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \text{true})];\ d_1 \rangle$.$\blacksquare$

- $*$ $S''(l) = (d_3, \text{true})$, where $d_3 \neq d_1$:

By Definition 3.2, $(d_1, \text{true}) \sqcup_p (d_3, \text{true}) = (\top, \text{false})$.

Therefore $S(l) \sqcup_p S''(l) = (\top, \text{false})$.

By Definition 3.1, $(\top, \text{false}) = \top_p$.

Therefore $S(l) \sqcup_p S''(l) = \top_p$.

Therefore, by Definition 3.5, $S \sqcup_S S'' = \top_S$.

This is a contradiction.

Therefore,

$$\langle S \sqcup_S S''; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, v, \{v \ldots\}, H\rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \text{true})];\ d_1\rangle. \blacksquare$$

In each case we have shown that

$\langle S \sqcup_S S''; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, v, \{v \ldots\}, H\rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \text{true})];\ d_1\rangle$.

Note that:

$$\begin{aligned}
(S \sqcup_S S'')[l \mapsto (d_1, \text{true})] &= S[l \mapsto (d_1, \text{true})] \sqcup_S S''[l \mapsto (d_1, \text{true})] \\
&= S \sqcup_S [l \mapsto (d_1, \text{true})] \sqcup_S S'' \sqcup_S [l \mapsto (d_1, \text{true})] \\
&= S \sqcup_S [l \mapsto (d_1, \text{true})] \sqcup_S S'' \\
&= S[l \mapsto (d_1, \text{true})] \sqcup_S S''.
\end{aligned}$$

Therefore

$\langle S \sqcup_S S''; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, v, \{v \ldots\}, H\rangle \hookrightarrow \langle S[l \mapsto (d_1, \text{true})] \sqcup_S S'';\ d_1\rangle$,

as we were required to show.

- Case E-Freeze-Simple:

  Given: $\langle S; \texttt{freeze}\, l\rangle \hookrightarrow \langle S[l \mapsto (d_1, \text{true})];\ d_1\rangle$.

  To show: $\langle S \sqcup_S S''; \texttt{freeze}\, l\rangle \hookrightarrow \langle S[l \mapsto (d_1, \text{true})] \sqcup_S S'';\ d_1\rangle$.

  We will first show that

  $\langle S \sqcup_S S''; \texttt{freeze}\, l\rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \text{true})];\ d_1\rangle$

  and then show why this is sufficient.

  We proceed by cases on l:

  - $l \notin \mathit{dom}(S'')$:

    By assumption, $S[l \mapsto (d_1, \text{true})] \sqcup_S S'' \neq \top_S$.

    By Lemma 3.3, $S \sqsubseteq_S S[l \mapsto (d_1, \text{true})]$.

    Therefore $S \sqcup_S S'' \neq \top_S$.

    Hence, by Definition 3.5, $(S \sqcup_S S'')(l) = S(l)$.

    From the premise of E-Freeze-Simple, we have that $S(l) = (d_1, \mathit{frz}_1)$.

    Therefore, by E-Freeze-Simple, we have that

    $\langle S \sqcup_S S''; \texttt{freeze}\, l\rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \text{true})];\ d_1\rangle$.

  - $l \in \mathit{dom}(S'')$:

    By assumption, $S[l \mapsto (d_1, \text{true})] \sqcup_S S'' \neq \top_S$.

By Lemma 3.3, $S \sqsubseteq_S S[l \mapsto (d_1, \text{true})]$.

Therefore $S \sqcup_S S'' \neq \top_S$.

Hence, by Definition 3.5, $(S \sqcup_S S'')(l) = S(l) \sqcup_p S''(l)$.

From the premise of E-Freeze-Simple, we have that $S(l) = (d_1, \mathit{frz}_1)$.

By assumption, $S[l \mapsto (d_1, \text{true})] \sqcup_S S'' =_{\mathit{frz}} S$.

Therefore $\mathit{frz}_1 = \text{true}$.

Therefore $(S \sqcup_S S'')(l) = (d_1, \text{true}) \sqcup_p S''(l)$.

We proceed by cases on $S''(l)$:

- $S''(l) = (d_2, \text{false})$, where $d_2 \sqsubseteq d_1$:

  By Definition 3.2, $(d_1, \text{true}) \sqcup_p (d_2, \text{false}) = (d_1, \text{true})$.

  Therefore $(S \sqcup_S S'')(l) = (d_1, \text{true})$.

  Therefore, by E-Freeze-Simple, we have that

  $\langle S \sqcup_S S''; \texttt{freeze}\ l \rangle \longleftrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \text{true})];\ d_1 \rangle$.

- $S''(l) = (d_2, \text{false})$, where $d_2 \not\sqsubseteq d_1$:

  By Definition 3.2, $(d_1, \text{true}) \sqcup_p (d_2, \text{false}) = (\top, \text{false})$.

  By Definition 3.1, $(\top, \text{false}) = \top_p$.

  Therefore $S(l) \sqcup_p S''(l) = \top_p$.

  Therefore, by Definition 3.5, $S \sqcup_S S'' = \top_S$.

  This is a contradiction.

  Therefore,

  $\langle S \sqcup_S S''; \texttt{freeze}\ l \rangle \longleftrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \text{true})];\ d_1 \rangle$.

- $S''(l) = (d_2, \text{true})$, where $d_2 = d_1$:

  Therefore $(S \sqcup_S S'')(l) = (d_1, \text{true}) \sqcup_p (d_2, \text{true})$.

  By Definition 3.2, $(d_1, \text{true}) \sqcup_p (d_2, \text{true}) = (d_1, \text{true})$.

  Therefore $(S \sqcup_S S'')(l) = (d_1, \text{true})$.

  Therefore, by E-Freeze-Simple, we have that

  $\langle S \sqcup_S S''; \texttt{freeze}\ l \rangle \longleftrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \text{true})];\ d_1 \rangle$.

- $S''(l) = (d_2, \text{true})$, where $d_2 \neq d_1$:

  By Definition 3.2, $(d_1, \text{true}) \sqcup_p (d_2, \text{true}) = (\top, \text{false})$.

By Definition 3.1, $(\top, \text{false}) = \top_p$.

Therefore $S(l) \sqcup_p S''(l) = \top_p$.

Therefore, by Definition 3.5, $S \sqcup_S S'' = \top_S$.

This is a contradiction.

Therefore,

$\langle S \sqcup_S S''; \ \texttt{freeze}\ l \rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \text{true})]; \ d_1 \rangle$.

In each case we have shown that

$\langle S \sqcup_S S''; \ \texttt{freeze}\ l \rangle \hookrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \text{true})]; \ d_1 \rangle$.

Note that:

$$\begin{aligned}(S \sqcup_S S'')[l \mapsto (d_1, \text{true})] &= S[l \mapsto (d_1, \text{true})] \sqcup_S S''[l \mapsto (d_1, \text{true})] \\ &= S \sqcup_S [l \mapsto (d_1, \text{true})] \sqcup_S S'' \sqcup_S [l \mapsto (d_1, \text{true})] \\ &= S \sqcup_S [l \mapsto (d_1, \text{true})] \sqcup_S S'' \\ &= S[l \mapsto (d_1, \text{true})] \sqcup_S S''.\end{aligned}$$

Therefore $\langle S \sqcup_S S''; \ \texttt{freeze}\ l \rangle \hookrightarrow \langle S[l \mapsto (d_1, \text{true})] \sqcup_S S''; \ d_1 \rangle$, as we were required to show.

□

A.11. Proof of Lemma 3.5

Proof. By induction on the derivation of $\sigma \hookrightarrow \sigma_a$, by cases on the last rule in the derivation.

- E-Eval-Ctxt: TODO: Figure out what to do here.
- E-Beta: $\sigma = \langle S; \ (\lambda x.\, e)\ v \rangle$, and $\sigma_a = \langle S; \ e[x := v] \rangle$.

  Given:

  - $\langle S; \ (\lambda x.\, e)\ v \rangle \hookrightarrow \langle S; \ e[x := v] \rangle$, and
  - $\langle S; \ (\lambda x.\, e)\ v \rangle \hookrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that

  $\langle S; \ e[x := v] \rangle \hookrightarrow^i \sigma_c$ and $\sigma_b \hookrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

  By inspection of the operational semantics, $\sigma_b = \langle S; \ e[x := v] \rangle$.

  Choose $\sigma_c = \langle S; \ e[x := v] \rangle$, $i = 0$ and $j = 0$.

Then $\langle S;\ e[x := v]\rangle = \sigma_c$ and $\sigma_b = \sigma_c$, as required.

- E-New: $\sigma = \langle S;\ \texttt{new}\rangle$, and $\sigma_a = \langle S[l \mapsto (\bot, \text{false})];\ l\rangle$.

  Given:

  - $\langle S;\ \texttt{new}\rangle \hookrightarrow \langle S[l \mapsto (\bot, \text{false})];\ l\rangle$, and
  - $\langle S;\ \texttt{new}\rangle \hookrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that

  $\langle S[l \mapsto (\bot, \text{false})];\ l\rangle \hookrightarrow^i \sigma_c$ and $\sigma_b \hookrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

  By inspection of the operational semantics, $\sigma_b = \langle S[l' \mapsto (\bot, \text{false})];\ l'\rangle$.

  From the side condition of E-New, $l \notin S$.

  Therefore, in $\langle S[l' \mapsto (\bot, \text{false})];\ l'\rangle$, we can α-rename l' to l, resulting in $\langle S[l \mapsto (\bot, \text{false})];\ l\rangle$.

  Choose $\sigma_c = \langle S[l \mapsto (\bot, \text{false})];\ l\rangle$, $i = 0$ and $j = 0$.

  Then $\langle S;\ e[x := v]\rangle = \sigma_c$ and $\sigma_b = \sigma_c$, as required.

- E-Put: $\sigma = \langle S;\ \texttt{put}\ l\ d_2\rangle$, and $\sigma_a = \langle S[l \mapsto p_2];\ \texttt{()}\rangle$.

  Given:

  - $\langle S;\ \texttt{put}\ l\ d_2\rangle \hookrightarrow \langle S[l \mapsto p_2];\ \texttt{()}\rangle$, and
  - $\langle S;\ \texttt{put}\ l\ d_2\rangle \hookrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that

  $\langle S[l \mapsto p_2];\ \texttt{()}\rangle \hookrightarrow^i \sigma_c$ and $\sigma_b \hookrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

  By inspection of the operational semantics, $\sigma_b = \langle S[l \mapsto p_2];\ \texttt{()}\rangle$.

  Choose $\sigma_c = \langle S[l \mapsto p_2];\ \texttt{()}\rangle$, $i = 0$ and $j = 0$.

  Then $\langle S[l \mapsto p_2];\ \texttt{()}\rangle = \sigma_c$ and $\sigma_b = \sigma_c$, as required.

- E-Put-Err: $\sigma = \langle S;\ \texttt{put}\ l\ d_2\rangle$, and $\sigma_a = \textbf{error}$.

  Given:

  - $\langle S;\ \texttt{put}\ l\ d_2\rangle \hookrightarrow \textbf{error}$, and
  - $\langle S;\ \texttt{put}\ l\ d_2\rangle \hookrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that

  error $\hookrightarrow^i \sigma_c$ and $\sigma_b \hookrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

  By inspection of the operational semantics, $\sigma_b = \textbf{error}$.

  Choose $\sigma_c = \textbf{error}$, $i = 0$ and $j = 0$.

Then **error** $= \sigma_c$ and $\sigma_b = \sigma_c$, as required.

- E-Get: $\sigma = \langle S;\, \texttt{get}\ l\ P \rangle$, and $\sigma_a = \langle S;\, p_2 \rangle$.

  Given:

  - $\langle S;\, \texttt{get}\ l\ P \rangle \hookrightarrow \langle S;\, p_2 \rangle$, and
  - $\langle S;\, \texttt{get}\ l\ P \rangle \hookrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that

  $\langle S;\, p_2 \rangle \hookrightarrow^i \sigma_c$ and $\sigma_b \hookrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

  By inspection of the operational semantics, $\sigma_b = \langle S;\, p_2 \rangle$.

  Choose $\sigma_c = \langle S;\, p_2 \rangle$, $i = 0$ and $j = 0$.

  Then $\langle S;\, p_2 \rangle = \sigma_c$ and $\sigma_b = \sigma_c$, as required.

- E-Freeze-Init: $\sigma = \langle S;\, \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e \rangle$, and $\sigma_a = \langle S;\, \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e, \{\}, \{\} \rangle$.

  Given:

  - $\langle S;\, \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\, e \rangle \hookrightarrow \langle S;\, \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\, e, \{\}, \{\} \rangle$, and
  - $\langle S;\, \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\, e \rangle \hookrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that

  $\langle S;\, \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\, e, \{\}, \{\} \rangle \hookrightarrow^i \sigma_c$ and $\sigma_b \hookrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

  By inspection of the operational semantics, $\sigma_b = \langle S;\, \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\, e, \{\}, \{\} \rangle$.

  Choose $\sigma_c = \langle S;\, \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\, e, \{\}, \{\} \rangle$, $i = 0$ and $j = 0$.

  Then $\langle S;\, \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\, e, \{\}, \{\} \rangle = \sigma_c$ and $\sigma_b = \sigma_c$, as required.

- E-Spawn-Handler: $\sigma = \langle S;\, \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\, e_0, \{e, \dots\}, H \rangle$, and $\sigma_a = \langle S;\, \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\, e_0, \{e_0[x := d_2], e, \dots\}, \{d_2\} \cup H \rangle$.

  Given:

  - $\langle S;\, \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\, e_0, \{e, \dots\}, H \rangle \hookrightarrow$
    $\langle S;\, \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\, e_0, \{e_0[x := d_2], e, \dots\}, \{d_2\} \cup H \rangle$, and
  - $\langle S;\, \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\, e_0, \{e, \dots\}, H \rangle \hookrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that

  $\langle S;\, \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\, e_0, \{e_0[x := d_2], e, \dots\}, \{d_2\} \cup H \rangle \hookrightarrow^i \sigma_c$ and $\sigma_b \hookrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

LK: This time, we could actually get different results on the two sides of the diamond because we could choose a different d_2, or we could run a different expression in $\{e, \ldots\}$.

By inspection of the operational semantics, one of the following possibilities must hold:

- $\sigma \hookrightarrow \sigma_b$ by E-Spawn-Handler:

  Hence $\sigma_b = \langle S; \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\, e_0, \{e_0[x := d_2'], e, \ldots\}, \{d_2'\} \cup H\rangle$.

  Here, there are two subcases:

  * $d_2' \neq d_2$:

    Choose:

    $\sigma_c = \langle S; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e_0[x := d_2'], e, \ldots\}, \{d_2, d_2'\} \cup H\rangle$,

    $i = 1$ and $j = 1$.

    To show:

    (1) $\sigma_a \hookrightarrow \sigma_c$, where

    $\sigma_a = \langle S; \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\, e_0, \{e_0[x := d_2], e, \ldots\}, \{d_2\} \cup H\rangle$ and

    $\sigma_c = \langle S; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e_0[x := d_2'], e, \ldots\}, \{d_2, d_2'\} \cup H\rangle$.

    The proof is as follows:

    From the premises of E-Spawn-Handler,

    $S(l) = (d_1, \mathit{frz}_1)$ and $d_2' \sqsubseteq d_1$ and $d_2' \notin H$ and $d_2' \in Q$.

    Therefore, by E-Spawn-Handler,

    $\langle S; \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\, e_0, \{e_0[x := d_2], e, \ldots\}, \{d_2\} \cup H\rangle \hookrightarrow$
    $\langle S; \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\, e_0, \{e_0[x := d_2'], e_0[x := d_2], e, \ldots\}, \{d_2'\} \cup \{d_2\} \cup H\rangle$,

    which is equivalent to

    $\langle S; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e_0[x := d_2'], e, \ldots\}, \{d_2, d_2'\} \cup H\rangle$.

    Hence $\sigma_a \hookrightarrow \sigma_c$.

(2) $\sigma_b \hookrightarrow \sigma_c$, where

$\sigma_b = \langle S;\, \texttt{freeze}\; l\; \texttt{after}\; Q\; \texttt{with}\; \lambda x.\, e_0, \{e_0[x := d_2'], e, \dots\}, \{d_2'\} \cup H\rangle$, and

$\sigma_c = \langle S;\, \texttt{freeze}\; l\; \texttt{after}\; Q\; \texttt{with}\; \lambda x.\, e_0, \{e_0[x := d_2], e_0[x := d_2'], e, \dots\}, \{d_2, d_2'\} \cup H\rangle$.

The proof is as follows:

From the premises of E-Spawn-Handler,

$S(l) = (d_1, \mathit{frz}_1)$ and $d_2 \sqsubseteq d_1$ and $d_2 \notin H$ and $d_2 \in Q$.

Therefore, by E-Spawn-Handler,

$\langle S;\, \texttt{freeze}\; l\; \texttt{after}\; Q\; \texttt{with}\; \lambda x.\, e_0, \{e_0[x := d_2'], e, \dots\}, \{d_2'\} \cup H\rangle \hookrightarrow$
$\langle S;\, \texttt{freeze}\; l\; \texttt{after}\; Q\; \texttt{with}\; \lambda x.\, e_0, \{e_0[x := d_2], e_0[x := d_2'], e, \dots\}, \{d_2\} \cup \{d_2'\} \cup H\rangle$,

which is equivalent to

$\langle S;\, \texttt{freeze}\; l\; \texttt{after}\; Q\; \texttt{with}\; \lambda x.\, e_0, \{e_0[x := d_2], e_0[x := d_2'], e, \dots\}, \{d_2, d_2'\} \cup H\rangle$.

Hence $\sigma_b \hookrightarrow \sigma_c$.

∗ $d_2' = d_2$:

Choose: $\sigma_c = \langle S;\, \texttt{freeze}\; l\; \texttt{after}\; Q\; \texttt{with}\; \lambda x.\, e_0, \{e_0[x := d_2], e, \dots\}, \{d_2\} \cup H\rangle$, $i = 0$ and $j = 0$.

Then $\langle S;\, \texttt{freeze}\; l\; \texttt{after}\; Q\; \texttt{with}\; \lambda x.\, e_0, \{e_0[x := d_2], e, \dots\}, \{d_2\} \cup H\rangle = \sigma_c$ and $\sigma_b = \sigma_c$, as required.

– $\sigma \hookrightarrow \sigma_b$ by E-Eval-Ctxt:

Hence $\sigma_b = \langle S';\, \texttt{freeze}\; l\; \texttt{after}\; Q\; \texttt{with}\; \lambda x.\, e_0, \{e', \dots\}, H\rangle$.

LK: Minor cheat here: the expression that could step could be *any* expression in the set $\{e, \dots\}$, not necessarily the first one. I'm hoping it's enough to just write out this case.

Choose:

$\sigma_c = \langle S';\, \texttt{freeze}\; l\; \texttt{after}\; Q\; \texttt{with}\; \lambda x.\, e_0, \{e_0[x := d_2], e', \dots\}, \{d_2\} \cup H\rangle$,

$i = 1$ and $j = 1$.

To show:

(1) $\sigma_a \hookrightarrow \sigma_c$, where

$\sigma_a = \langle S;\, \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e, \ldots\}, \{d_2\} \cup H\rangle$ and

$\sigma_c = \langle S';\, \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e', \ldots\}, \{d_2\} \cup H\rangle$.

The proof is as follows:

From the premise of E-Eval-Ctxt, $\langle S;\, e\rangle \hookrightarrow \langle S';\, e'\rangle$.

From the definition of evaluation contexts,

$\texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], [\,], \ldots\}, \{d_2\} \cup H$

is an evaluation context.

Hence, by E-Eval-Ctxt,

$\langle S;\, \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e, \ldots\}, \{d_2\} \cup H\rangle \hookrightarrow$

$\langle S';\, \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e', \ldots\}, \{d_2\} \cup H\rangle$.

Hence $\sigma_a \hookrightarrow \sigma_c$.

(2) $\sigma_b \hookrightarrow \sigma_c$, where

$\sigma_b = \langle S';\, \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e', \ldots\}, H\rangle$, and

$\sigma_c = \langle S';\, \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e', \ldots\}, \{d_2\} \cup H\rangle$.

The proof is as follows:

From the premises of E-Spawn-Handler,

$S(l) = (d_1, \mathit{frz}_1)$ and $d_2 \sqsubseteq d_1$ and $d_2 \notin H$ and $d_2 \in Q$.

Hence, by E-Spawn-Handler,

$\langle S';\, \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e', \ldots\}, H\rangle \hookrightarrow$

$\langle S';\, \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e', \ldots\}, \{d_2\} \cup H\rangle$.

Hence $\sigma_b \hookrightarrow \sigma_c$.

- E-Freeze-Final: $\sigma = \langle S;\, \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, v, \{v \ldots\}, H\rangle$, and $\sigma_a = \langle S[l \mapsto (d_1, \text{true})];\, d_1\rangle$.█

  Given:

  - $\langle S;\, \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, v, \{v \ldots\}, H\rangle \hookrightarrow \langle S[l \mapsto (d_1, \text{true})];\, d_1\rangle$, and
  - $\langle S;\, \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, v, \{v \ldots\}, H\rangle \hookrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that

  $\langle S[l \mapsto (d_1, \text{true})];\, d_1\rangle \hookrightarrow^i \sigma_c$ and $\sigma_b \hookrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

  By inspection of the operational semantics, $\sigma_b = \langle S[l \mapsto (d_1, \text{true})];\, d_1\rangle$.

Choose $\sigma_c = \langle S[l \mapsto (d_1, \text{true})];\ d_1\rangle$, $i = 0$ and $j = 0$.

Then $\langle S[l \mapsto (d_1, \text{true})];\ d_1\rangle = \sigma_c$ and $\sigma_b = \sigma_c$, as required.

- E-Freeze-Simple: $\sigma = \langle S;\ \texttt{freeze}\ l\rangle$, and $\sigma_a = \langle S[l \mapsto (d_1, \text{true})];\ d_1\rangle$.

  Given:

  - $\langle S;\ \texttt{freeze}\ l\rangle \hookrightarrow \langle S[l \mapsto (d_1, \text{true})];\ d_1\rangle$, and
  - $\langle S;\ \texttt{freeze}\ l\rangle \hookrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that $\langle S[l \mapsto (d_1, \text{true})];\ d_1\rangle \hookrightarrow^i \sigma_c$ and $\sigma_b \hookrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

  By inspection of the operational semantics, $\sigma_b = \langle S[l \mapsto (d_1, \text{true})];\ d_1\rangle$.

  Choose $\sigma_c = \langle S[l \mapsto (d_1, \text{true})];\ d_1\rangle$, $i = 0$ and $j = 0$.

  Then $\langle S[l \mapsto (d_1, \text{true})];\ d_1\rangle = \sigma_c$ and $\sigma_b = \sigma_c$, as required.

□

A.12. Proof of Lemma 3.6

Proof. We proceed by induction on m. In the base case of $m = 1$, the result is immediate from Lemma 3.5, with $k = 1$.

For the induction step, suppose $\sigma \hookrightarrow^m \sigma'' \hookrightarrow \sigma'''$ and suppose the lemma holds for m.

We show that it holds for $m + 1$, as follows.

We are required to show that either:

(1) there exist σ_c, i, j such that $\sigma' \hookrightarrow^i \sigma_c$ and $\sigma''' \hookrightarrow^j \sigma_c$ and $i \leq m + 1$ and $j \leq 1$, or
(2) there exists $k \leq m + 1$ such that $\sigma' \hookrightarrow^k$ **error**, or there exists $k \leq 1$ such that $\sigma''' \hookrightarrow^k$ **error**.

From the induction hypothesis, we have that either:

(1) there exist σ'_c, i', j' such that $\sigma' \hookrightarrow^{i'} \sigma'_c$ and $\sigma'' \hookrightarrow^{j'} \sigma'_c$ and $i' \leq m$ and $j' \leq 1$, or
(2) there exists $k' \leq m$ such that $\sigma' \hookrightarrow^{k'}$ **error**, or there exists $k' \leq 1$ such that $\sigma'' \hookrightarrow^{k'}$ **error**.

We consider these two cases in turn:

(1) There exist σ'_c, i', j' such that $\sigma' \hookrightarrow^{i'} \sigma'_c$ and $\sigma'' \hookrightarrow^{j'} \sigma'_c$ and $i' \leq m$ and $j' \leq 1$:

   LK: This gets very hairy. I could spell things out in more detail, but it's MUCH better explained with a drawing, which I'm happy to do later. :)

   We proceed by cases on j':

   - If $j' = 0$, then $\sigma'' = \sigma'_c$. We can then choose $\sigma_c = \sigma'''$ and $i = i' + 1$ and $j = 0$.
   - If $j' = 1$:

     From $\sigma'' \hookrightarrow \sigma'''$ and $\sigma'' \hookrightarrow^{j'} \sigma'_c$ and Lemma 3.5, one of the following two cases is true:

     (a) There exist σ''_c and i'' and j'' such that $\sigma'_c \hookrightarrow^{i''} \sigma''_c$ and $\sigma''' \hookrightarrow^{j''} \sigma''_c$ and $i'' \leq 1$ and $j'' \leq 1$. So we also have $\sigma' \hookrightarrow^{i'} \sigma'_c \hookrightarrow^{i''} \sigma''_c$. In summary, we pick $\sigma_c = \sigma''_c$ and $i = i' + i''$ and $j = j''$, which is sufficient because $i = i' + i'' \leq m + 1$ and $j = j'' \leq 1$.

     (b) $\sigma''' \hookrightarrow$ **error** or $\sigma'_c \hookrightarrow$ **error**.

     If $\sigma''' \hookrightarrow$ **error**, then choosing $k = 1$ satisfies the proof.

     Otherwise, $\sigma'_c \hookrightarrow$ **error**, therefore $\sigma' \hookrightarrow^{i'} \sigma'_c \hookrightarrow$ **error**.

     Hence $\sigma' \hookrightarrow^{i'+1}$ **error**.

     Since $i' \leq m$, we have that $i' + 1 \leq m + 1$, and so choosing $k = i' + 1$ satisfies the proof.

(2) There exists $k' \leq m$ such that $\sigma' \hookrightarrow^{k'}$ **error**, or there exists $k' \leq 1$ such that $\sigma'' \hookrightarrow^{k'}$ **error**:

   If there exists $k' \leq m$ such that $\sigma' \hookrightarrow^{k'}$ **error**, then choosing $k = k'$ satisfies the proof.

   Otherwise, there exists $k' \leq 1$ such that $\sigma'' \hookrightarrow^{k'}$ **error**. We proceed by cases on k':

   - If $k' = 0$, then $\sigma'' =$ **error**.

     Hence this case is not possible, since $\sigma'' \hookrightarrow \sigma'''$ and **error** cannot step.
   - If $k' = 1$:

     From $\sigma'' \hookrightarrow \sigma'''$ and $\sigma'' \hookrightarrow^{k'}$ **error** and Lemma 3.5, one of the following two cases is true:

     (a) There exist σ''_c and i'' and j'' such that **error** $\hookrightarrow^{i''} \sigma''_c$ and $\sigma''' \hookrightarrow^{j''} \sigma''_c$ and $i'' \leq 1$ and $j'' \leq 1$.

     Since **error** cannot step, $i'' = 0$ and $\sigma''_c =$ **error**.

     Hence $\sigma''' \hookrightarrow^{j''}$ **error**.

     LK: This is the one place that we need to allow k to be ≤ 1 instead of exactly 1.

     Since $j'' \leq 1$, choosing $k = j''$ satisfies the proof.

(b) **error** $\hookrightarrow$ **error** or $\sigma''' \hookrightarrow$ **error**.

Since **error** cannot step, $\sigma''' \hookrightarrow$ **error**.

Hence choosing $k = 1$ satisfies the proof.

□

A.13. Proof of Lemma 3.7

Proof. We proceed by induction on n. In the base case of $n = 1$, the result is immediate from Lemma 3.6.

For the induction step, suppose $\sigma \hookrightarrow^{n} \sigma' \hookrightarrow \sigma'''$ and suppose the lemma holds for n.

We show that it holds for $n + 1$, as follows.

We are required to show that either:

(1) there exist σ_c, i, j such that $\sigma''' \hookrightarrow^{i} \sigma_c$ and $\sigma'' \hookrightarrow^{j} \sigma_c$ and $i \leq m$ and $j \leq n + 1$, or

(2) there exists $k \leq m$ such that $\sigma''' \hookrightarrow^{k}$ **error**, or there exists $k \leq n+1$ such that $\sigma'' \hookrightarrow^{k}$ **error**.

From the induction hypothesis, we have that either:

(1) there exist σ'_c, i', j' such that $\sigma' \hookrightarrow^{i'} \sigma'_c$ and $\sigma'' \hookrightarrow^{j'} \sigma'_c$ and $i' \leq m$ and $j' \leq n$, or

(2) there exists $k' \leq m$ such that $\sigma' \hookrightarrow^{k'}$ **error**, or there exists $k' \leq n$ such that $\sigma'' \hookrightarrow^{k'}$ **error**.

We consider these two cases in turn:

(1) There exist σ'_c, i', j' such that $\sigma' \hookrightarrow^{i'} \sigma'_c$ and $\sigma'' \hookrightarrow^{j'} \sigma'_c$ and $i' \leq m$ and $j' \leq n$:

We proceed by cases on i':

- If $i' = 0$, then $\sigma' = \sigma'_c$. We can then choose $\sigma_c = \sigma'''$ and $i = 0$ and $j = j' + 1$.
- If $i' \geq 1$:

  From $\sigma' \hookrightarrow \sigma'''$ and $\sigma' \hookrightarrow^{i'} \sigma'_c$ and Lemma 3.6, one of the following two cases is true:

  (a) There exist σ''_c and i'' and j'' such that $\sigma''' \hookrightarrow^{i''} \sigma''_c$ and $\sigma'_c \hookrightarrow^{j''} \sigma''_c$ and $i'' \leq i'$ and $j'' \leq 1$. So we also have $\sigma'' \hookrightarrow^{j'} \sigma'_c \hookrightarrow^{j''} \sigma''_c$. In summary, we pick $\sigma_c = \sigma''_c$ and $i = i''$ and $j = j' + j''$, which is sufficient because $i = i'' \leq i' \leq m$ and $j = j' + j'' \leq n + 1$.

(b) There exists $k'' \leq i'$ such that $\sigma''' \hookrightarrow^{k''}$ **error**, or there exists $k'' \leq 1$ such that $\sigma'_c \hookrightarrow^{k''}$ **error**.

If there exists $k'' \leq i'$ such that $\sigma''' \hookrightarrow^{k''}$ **error**, then choosing $k = k''$ satisfies the proof, since $k'' \leq i' \leq m$.

Otherwise, there exists $k'' \leq 1$ such that $\sigma'_c \hookrightarrow^{k''}$ **error**.

Therefore, $\sigma'' \hookrightarrow^{j'} \sigma'_c \hookrightarrow^{k''}$ **error**.

Hence $\sigma'' \hookrightarrow^{j'+k''}$ **error**.

Since $j' \leq n$ and $k'' \leq 1$, $j' + k'' \leq n + 1$.

Hence choosing $k = j' + k''$ satisfies the proof.

(2) There exists $k' \leq m$ such that $\sigma' \hookrightarrow^{k'}$ **error**, or there exists $k' \leq n$ such that $\sigma'' \hookrightarrow^{k'}$ **error**:

If there exists $k' \leq n$ such that $\sigma'' \hookrightarrow^{k'}$ **error**, then choosing $k = k'$ satisfies the proof.

Otherwise, there exists $k' \leq m$ such that $\sigma' \hookrightarrow^{k'}$ **error**. We proceed by cases on k':

- If $k' = 0$, then $\sigma' =$ **error**.

  Hence this case is not possible, since $\sigma' \hookrightarrow \sigma'''$ and **error** cannot step.

- If $k' \geq 1$:

  From $\sigma' \hookrightarrow \sigma'''$ and $\sigma' \hookrightarrow^{k'}$ **error** and Lemma 3.6, one of the following two cases is true:

  (a) There exist σ''_c and i'' and j'' such that $\sigma''' \hookrightarrow^{i''} \sigma''_c$ and **error** $\hookrightarrow^{j''} \sigma''_c$ and $i'' \leq k'$ and $j'' \leq 1$.

  Since **error** cannot step, $j'' = 0$ and $\sigma''_c =$ **error**.

  Hence $\sigma''' \hookrightarrow^{i''}$ **error**.

  Since $i'' \leq k' \leq m$, choosing $k = i''$ satisfies the proof.

  (b) There exists $k'' \leq k'$ such that $\sigma''' \hookrightarrow^{k''}$ **error**, or there exists $k'' \leq 1$ such that **error** $\hookrightarrow^{k''}$ **error**.

  Since **error** cannot step, there exists $k'' \leq k'$ such that $\sigma''' \hookrightarrow^{k''}$ **error**.

  Since $k'' \leq k' \leq m$, choosing $k = k''$ satisfies the proof.

□

APPENDIX B

PLT Redex Models of λ_{LVar} and λ_{LVish}

TODO: Edit this text.

We have developed a runnable version of the LVish calculus[1] using the PLT Redex semantics engineering toolkit [**18**]. In the Redex of today, it is not possible to directly parameterize a language definition by a lattice.[2] Instead, taking advantage of Racket's syntactic abstraction capabilities, we define a Racket macro, `define-LVish-language`, that wraps a template implementing the lattice-agnostic semantics of Figure **??**, and takes the following arguments:

- a *name*, which becomes the *lang-name* passed to Redex's `define-language` form;
- a *"downset" operation*, a Racket-level procedure that takes a lattice element and returns the (finite) set of all lattice elements that are below that element (this operation is used to implement the semantics of `freeze` − `after` − `with`, in particular, to determine when the E-Freeze-Final rule can fire);
- a *lub operation*, a Racket-level procedure that takes two lattice elements and returns a lattice element; and
- a (possibly infinite) set of *lattice elements* represented as Redex *patterns*.

Given these arguments, `define-LVish-language` generates a Redex model specialized to the application-specific lattice in question. For instance, to instantiate a model called `nat`, where the application-specific lattice is the natural numbers with `max` as the least upper bound, one writes:

```
(define-LVish-language nat downset-op max natural)
```

[1] Available at `http://github.com/iu-parfunc/lvars`.

[2] See discussion at `http://lists.racket-lang.org/users/archive/2013-April/057075.html`.

where downset-op is separately defined. Here, downset-op and max are Racket procedures. natural is a Redex pattern that has no meaning to Racket proper, but because define-LVish-language is a macro, natural is not evaluated until it is in the context of Redex.LK: This might be too much information, or a little confusing. It's a nice illustration of the power of macros, though. I'd welcome suggestions for how to word it differently.

TODO: Freshen up the Redex models of λ_{LVar} and λ_{LVish} and add them here.