Freeze After Writing:
Quasi-Deterministic Parallel Programming with LVars

Lindsey Kuper   Aaron Turon   Neelakantan R. Krishnaswami   Ryan R. Newton

November 2013

Abstract

Deterministic-by-construction parallel programming models offer the advantages of parallel speedup while avoiding the nondeterministic, hard-to-reproduce bugs that plague fully concurrent code. A principled approach to deterministic-by-construction parallel programming with shared state is offered by *LVars*: shared memory locations whose semantics are defined in terms of an application-specific lattice. Writes to an LVar take the least upper bound of the old and new values with respect to the lattice, while reads from an LVar can observe only that its contents have crossed a specified threshold in the lattice. Although it guarantees determinism, this interface is quite limited.

We extend LVars in two ways. First, we add the ability to "freeze" and then read the contents of an LVar directly. Second, we add the ability to attach event handlers to an LVar, triggering a callback when the LVar's value changes. Together, handlers and freezing enable an expressive and useful style of parallel programming. We prove that in a language where communication takes place through these extended LVars, programs are at worst *quasi-deterministic*: on every run, they either produce the same answer or raise an error. We demonstrate the viability of our approach by implementing a library for Haskell supporting a variety of LVar-based data structures, together with a case study that illustrates the programming model and yields promising parallel speedup.

1   Introduction

Flexible parallelism requires tasks to be scheduled dynamically, in response to the vagaries of an execution. But if the resulting schedule nondeterminism is *observable* within a program, it becomes much more difficult for programmers to discover and correct bugs by testing, let alone to reason about their code in the first place.

While much work has focused on identifying methods of deterministic parallel programming [8, 22, 6, 19, 21, 32], *guaranteed* determinism in real parallel programs remains a lofty and rarely achieved goal. It places stringent constraints on the programming model: concurrent tasks must communicate in restricted ways that prevent them from observing the effects of scheduling, a restriction that must be enforced at the language or runtime level.

The simplest strategy is to allow *no* communication, forcing concurrent tasks to produce values independently. Pure data-parallel languages follow this strategy [28], as do languages that force references to be either task-unique or immutable [6]. But some algorithms are more naturally or efficiently written using shared state or message passing. A variety of deterministic-by-construction models allow limited communication along these lines, but they tend to be narrow in scope and permit communication through only a single data structure: for instance, FIFO queues in Kahn process networks [19] and StreamIt [17], or shared write-only tables in Intel Concurrent Collections [8].

Big-tent deterministic parallelism   Our goal is to create a broader, general-purpose deterministic-by-construction programming environment to increase the appeal and applicability of the method. We seek an approach that is not tied to a particular data structure and that supports familiar idioms from both functional and imperative programming styles. Our starting point is 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.

Our recently proposed *LVars* programming model [20] makes an initial foray into programming with monotonic data structures. In this model (which we review in Section 2), 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 *join* (least upper bound) 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, supports an unlimited variety of data structures (anything viewable as a lattice), and provides a familiar API, so it already achieves several of our goals. Unfortunately, it is not as general-purpose as one might hope.

Consider an 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 read and least-upper-bound write operations described above.

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.

Monotonic data structures that can say "no"   In this paper, we propose two additions to the LVars model that significantly extend its reach.

First, we add *event handlers*, a mechanism for attaching a callback function to an LVar that runs, 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.

Second, we add a primitive 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.[1]

Putting these features together, we can write a parallel graph traversal algorithm 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 our Haskell implementation (described in Section 6),[2] 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. 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. The `freezeSetAfter` function combines the constructs proposed above. First, it installs 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.

---

[1]Our original work on LVars [20] included a brief sketch of a similar proposal for a "consume" operation on LVars, but did not study it in detail. Here, we include freezing in our model, prove quasi-determinism for it, and show how to program with it in conjunction with our other proposal, handlers.

[2]The `Par` type constructor is the monad in which LVar computations live.

Quasi-determinism Unfortunately, freezing does not commute with writes that change an LVar.[3] 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 we 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. In our proposed model, this exception can in principle pinpoint the exact pair of freeze and write operations that are racing, greatly easing debugging.

Our general observation is that *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 small distance into nondeterminism, and make our way back. The identification of quasi-deterministic programs as a useful intermediate class is a contribution of this paper. That said, in many cases our freezing 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, we can guarantee determinism, since no writes can subsequently occur.

Contributions The technical contributions of this paper are:

- We introduce *LVish*, a quasi-deterministic parallel programming model that extends LVars to incorporate freezing and event handlers (Section 3). In addition to our high-level design, we present a core calculus for LVish (Section 4), formalizing its semantics, and include a runnable version, implemented in PLT Redex (Section 4.7), for interactive experimentation.

- We give a proof of quasi-determinism for the LVish calculus (Section 5). The key lemma, Independence, gives a kind of *frame property* for LVish computations: very roughly, if a computation takes an LVar from state p to p', then it would take the same LVar from the state $p \sqcup p_F$ to $p' \sqcup p_F$. The Independence lemma captures the commutative effects of LVish computations.

- We describe a Haskell library for practical quasi-deterministic parallel programming based on LVish (Section 6). 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 to be used safely with a fully-deterministic index.

- In Section 7, we evaluate our library with a case study: parallelizing control flow analysis. The case study begins with an existing implementation of k-CFA [26] 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.

2 Background: the LVars Model

IVars [1, 27, 8, 24] are a well-known mechanism for deterministic parallel programming. An IVar is a *single-assignment* variable [32] with a blocking read semantics: an attempt to read an empty IVar will block until the IVar has been filled with a value. We recently proposed *LVars* [20] as 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.

---

[3]The same is true for quiescence detection; see Section 3.2.

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

$$\texttt{let par } \_ = \texttt{put } lv\ 3$$
$$\_ = \texttt{put } lv\ 2 \qquad \text{(Example 1)}$$
$$\texttt{in get } lv$$

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

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

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 1(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 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 1(b), in which the least upper bound of any two distinct positive integers is $\top$, then Example 1 will deterministically raise an exception, indicating that conflicting writes to lv have occurred. This exception is analogous to the "multiple `put`" error raised 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.

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 1(a) for lv, but suppose we change Example 1 to allow the `get` operation to be interleaved with the two `put`s:

$$\texttt{let par } \_ = \texttt{put } lv\ 3$$
$$\_ = \texttt{put } lv\ 2$$
$$x = \texttt{get } lv \qquad \text{(Example 2)}$$
$$\texttt{in } x$$

Since the two `put`s and the `get` can be scheduled in any order, Example 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 behave deterministically by passing a threshold set argument to `get`. 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.
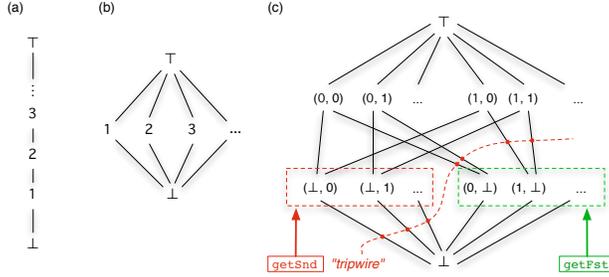
Figure 1: Example LVar lattices: (a) positive integers ordered by $\leq$; (b) IVar containing a positive integer; (c) pair of natural-number-valued IVars, annotated with example threshold sets that would correspond to a blocking read of the first or second element of the pair. Any state transition crossing the "tripwire" for `getSnd` causes it to unblock and return a result.

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 $\perp$ and may each be updated once with a non-$\perp$ value, which must be some natural number. This lattice is shown in Figure 1(c).

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

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

This allows us to write programs like the following:

$$
\begin{aligned}
\texttt{let par}\, \_ &= \texttt{put}\, lv\, (\perp, 4) \\
\_ &= \texttt{put}\, lv\, (3, \perp) \\
x &= \texttt{getSnd}\, lv \\
\texttt{in}\, x &
\end{aligned}
$$

(Example 3)

In the call `getSnd` lv, the threshold set is $\{(\perp, 0), (\perp, 1), \ldots\}$, 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 $\{(\perp, 0), (\perp, 1), \ldots\}$ can ever be reached. (We formalize this incompatibility requirement in Section 4.5.)

In the case of Example 3, `getSnd` lv may unblock and return $(\perp, 4)$ 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.

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. Our library (discussed in Section 6) 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.

3   LVish, Informally

As we explained in Section 1, 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, we explain our extensions to the LVar model at a high level; Section 4 then formalizes them, while Section 6 shows how to implement them.

3.1   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. For example, if lv is an LVar whose lattice is that of Figure 1(a), the expression

$$\texttt{addHandler}\ lv\ \{1, 3, 5, \dots\}\ (\lambda x.\,\texttt{put}\ lv\ x + 1) \tag{Example 4}$$

registers a handler for lv that executes the callback function $\lambda x.\,\texttt{put}\ lv\ x + 1$ for each odd number that lv is at or above. When Example 4 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` is an arbitrary subset Q of the LVar's lattice, specifying which events should be handled. Like threshold sets, these *event sets* are a mathematical modeling tool only; they have no explicit existence in the implementation.

Event handlers in LVish 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:

$$
\begin{aligned}
&\texttt{let par}\ \_ = \texttt{put}\ lv\ 0 \\
&\qquad\quad \_ = \texttt{put}\ lv\ 1 \\
&\qquad\quad \_ = \texttt{addHandler}\ lv\ \{0, 1\}\ (\lambda x.\,\texttt{if}\ x = 0\ \texttt{then}\ \texttt{put}\ lv\ 2) \\
&\quad \texttt{in get}\ lv\ \{2\}
\end{aligned}
\tag{Example 5}
$$

Can Example 5 ever block? If a callback only executed for events that arrived after its handler was registered, or only for the largest event in its handler 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 `put`s. 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 5, 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:

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

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 7.

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 6.2, we will see that this kind of handler set can be specified in a lattice-generic way, and in Section 6 we will see that it corresponds closely to our implementation strategy.

3.2 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 discussed in Section 1, 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 use a handler pool is 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 `addInPool`, a variant of `addHandler` that takes a handler pool as an additional argument. Finally, `quiesce` blocks until a pool of handlers has 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 `put`s 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 `put`s will not arrive to increase the state and trigger more callbacks. There is 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 we explain next.

3.3 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. As we explained in Section 1, `put`s that would change the value of a frozen LVar instead raise an exception, and it is the potential for races between such `put`s and `freeze` that makes LVish quasi-deterministic, rather than fully deterministic.

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

```
freezeAfter = λlv. λQ. λf.  let h = newPool
                              in addInPool h lv Q f;
                                   quiesce h; freeze lv
```

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. A set-specific variant of this pattern, `freezeSetAfter`, was used in the graph traversal example in Section 1.

4 LVish, Formally

In this section, we present a core calculus for LVish—in particular, a quasi-deterministic, parallel, call-by-value λ-calculus extended with a store containing LVars. It extends the original LVar formalism to support event handlers and freezing. In comparison to the informal description given in the last two sections, we make two simplifications to keep the model lightweight:

- We parameterize the definition of the LVish calculus by a *single* application-specific lattice, representing the set of states that LVars in the calculus can take on. Therefore 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, we instead formalize the "freeze-after" pattern—which combined them—directly as a primitive. This greatly simplifies the calculus, while still capturing the essence of our programming model.

In this section we cover the most important aspects of the LVish core calculus. Complete details, including the proof of Lemma 1, are given in Appendix A.

4.1 Lattices

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. We require that every two elements of D 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 ($\top$). For brevity, we use the term "lattice" as shorthand for "bounded join-semilattice with a designated greatest element" in the rest of this paper. We also occasionally use D as a shorthand for the entire 4-tuple $(D, \sqsubseteq, \bot, \top)$ when its meaning is clear from the context.

4.2 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 our model an LVar's *state* is a pair (d, frz), where d is an element of the application-specific set D and frz is a "status bit" of either true or false. We can define an ordering $\sqsubseteq_p$ on LVar states (d, 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, $(d, \mathsf{false}) \sqsubseteq_p (d', \mathsf{false})$ exactly when $d \sqsubseteq d'$.

- Two frozen states do not have an order, unless they are equal: $(d, \mathsf{true}) \sqsubseteq_p (d', \mathsf{true})$ 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, $(d, \mathsf{true}) \sqsubseteq_p (d', \mathsf{false})$ exactly when $d' = \top$.

The addition of status bits to the application-specific lattice results in a new lattice $(D_p, \sqsubseteq_p, \bot_p, \top_p)$, and we write $\sqcup_p$ for the least upper bound operation that $\sqsubseteq_p$ induces. Definition 1 and Lemma 1 formalize this notion.

Definition 1 (Lattice freezing). Suppose $(D, \sqsubseteq, \bot, \top)$ is a lattice. We define an operation $\mathrm{Freeze}(D, \sqsubseteq, \bot, \top) \triangleq (D_p, \sqsubseteq_p, \bot_p, \top_p)$ as follows:

1. D_p is a set defined as follows:

$$D_p \triangleq \{(d, frz) \mid d \in (D - \{\top\}) \land frz \in \{\mathsf{true}, \mathsf{false}\}\}$$
$$\cup \{(\top, \mathsf{false})\}$$

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

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

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

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

Lemma 1 (Lattice structure). *If $(D, \sqsubseteq, \bot, \top)$ is a lattice then* $\mathrm{Freeze}(D, \sqsubseteq, \bot, \top)$ *is as well.*

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

$$
\begin{array}{rl}
\text{configurations } \sigma & ::= \langle S; e \rangle \mid \textbf{error} \\
\text{expressions } e & ::= x \mid v \mid e\,e \mid \mathtt{get}\,e\,e \mid \mathtt{put}\,e\,e \mid \mathtt{new} \mid \mathtt{freeze}\,e \\
& \mid\ \mathtt{freeze}\,e\ \mathtt{after}\,e\ \mathtt{with}\,e \\
& \mid\ \mathtt{freeze}\,l\ \mathtt{after}\,Q\ \mathtt{with}\,\lambda x.e, \{e, \ldots\}, H \\
\text{stores } S & ::= [l_1 \mapsto p_1, \ldots, l_n \mapsto p_n] \mid \top_S \\
\text{values } v & ::= () \mid d \mid p \mid l \mid P \mid Q \mid \lambda x.e \\
\text{eval contexts } E & ::= [\,] \mid E\,e \mid e\,E \mid \mathtt{get}\,E\,e \mid \mathtt{get}\,e\,E \mid \mathtt{put}\,E\,e \\
& \mid\ \mathtt{put}\,e\,E \mid \mathtt{freeze}\,E \mid \mathtt{freeze}\,E\ \mathtt{after}\,e\ \mathtt{with}\,e \\
& \mid\ \mathtt{freeze}\,e\ \mathtt{after}\,E\ \mathtt{with}\,e \mid \mathtt{freeze}\,e\ \mathtt{after}\,e\ \mathtt{with}\,E \\
& \mid\ \mathtt{freeze}\,v\ \mathtt{after}\,v\ \mathtt{with}\,v, \{e\ldots E\,e\ldots\}, H
\end{array}
$$

$$
\begin{array}{ll}
\text{``handled'' sets } H ::= \{d_1, \ldots, d_n\} & \\
\text{threshold sets } P ::= \{p_1, p_2, \ldots\} & \text{states } p\ ::= (d, \mathit{frz}) \\
\text{event sets } Q ::= \{d_1, d_2, \ldots\} & \text{status bits } \mathit{frz} ::= \mathsf{true} \mid \mathsf{false}
\end{array}
$$

Figure 2: Syntax for LVish.

4.3 Stores

During the evaluation of 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.

Definition 2. A *store* is either a finite partial mapping $S : Loc \xrightarrow{\text{fin}} (D_p - \{\top_p\})$, or the distinguished element $\top_S$.

We 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. We can also denote a store by explicitly writing out all its bindings, using the notation $[l_1 \mapsto (d_1, \mathit{frz}_1), l_2 \mapsto (d_2, \mathit{frz}_2), \ldots]$.

It is straightforward to lift the $\sqsubseteq_p$ operations defined on elements of D_p to the level of stores:

Definition 3. 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 $l \in \mathit{dom}(S)$, $S(l) \sqsubseteq_p S'(l)$.

Stores ordered by $\sqsubseteq_S$ also form a lattice (with bottom element $\emptyset$ and top element $\top_S$); we write $\sqcup_S$ for the induced lub operation (concretely defined in Appendix B). If, for example,

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

then

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

A store containing a binding $l \mapsto (\top, \mathit{frz})$ can never arise during the execution of an LVish program, because, as we will see in Section 4.5, an attempted $\mathtt{put}$ that would take the value of l to $\top$ will raise an error.

4.4 The LVish Calculus

The syntax and operational semantics of the LVish calculus appear in Figures 2 and 3, respectively. As we have noted, both the syntax and semantics are parameterized by the lattice $(D, \sqsubseteq, \bot, \top)$. The reduction relation $\longrightarrow$ 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 we consider $\langle \top_S; e \rangle$ to be equal to **error** for all expressions e. The metavariable σ ranges over configurations.

9

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

$incomp(P) \triangleq \forall p_1, p_2 \in P. \ (p_1 \neq p_2 \implies p_1 \sqcup_p p_2 = \top_p)$

$$\boxed{\sigma \longrightarrow \sigma'}$$

E-EVAL-CTXT
$$\frac{\langle S; e \rangle \longrightarrow \langle S'; e' \rangle}{\langle S; E[e] \rangle \longrightarrow \langle S'; E[e'] \rangle}$$

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

E-NEW
$$\frac{}{\langle S; \texttt{new} \rangle \longrightarrow \langle S[l \mapsto (\bot, \textsf{false})]; l \rangle} \ (l \notin dom(S))$$

E-PUT
$$\frac{S(l) = p_1 \qquad p_2 = p_1 \sqcup_p (d_2, \textsf{false}) \qquad p_2 \neq \top_p}{\langle S; \texttt{put} \ l \ d_2 \rangle \longrightarrow \langle S[l \mapsto p_2]; \ () \rangle}$$

E-PUT-ERR
$$\frac{S(l) = p_1 \qquad p_1 \sqcup_p (d_2, \textsf{false}) = \top_p}{\langle S; \texttt{put} \ l \ d_2 \rangle \longrightarrow \textbf{error}}$$

E-GET
$$\frac{S(l) = p_1 \qquad incomp(P) \qquad p_2 \in P \qquad p_2 \sqsubseteq_p p_1}{\langle S; \texttt{get} \ l \ P \rangle \longrightarrow \langle S; p_2 \rangle}$$

E-FREEZE-INIT
$$\frac{}{\langle S; \texttt{freeze} \ l \ \texttt{after} \ Q \ \texttt{with} \ \lambda x. e \rangle \longrightarrow \langle S; \texttt{freeze} \ l \ \texttt{after} \ Q \ \texttt{with} \ \lambda x. e, \{\}, \{\} \rangle}$$

E-SPAWN-HANDLER
$$\frac{S(l) = (d_1, frz_1) \qquad d_2 \sqsubseteq d_1 \qquad d_2 \notin H \qquad d_2 \in Q}{\langle S; \texttt{freeze} \ l \ \texttt{after} \ Q \ \texttt{with} \ \lambda x. e_0, \{e, \dots\}, H \rangle \longrightarrow \langle S; \texttt{freeze} \ l \ \texttt{after} \ Q \ \texttt{with} \ \lambda x. e_0, \{e_0[x := d_2], e, \dots\}, \{d_2\} \cup H \rangle}$$

E-FREEZE-FINAL
$$\frac{S(l) = (d_1, frz_1) \qquad \forall d_2 . \ (d_2 \sqsubseteq d_1 \wedge d_2 \in Q \Rightarrow d_2 \in H)}{\langle S; \texttt{freeze} \ l \ \texttt{after} \ Q \ \texttt{with} \ v, \{v \dots\}, H \rangle \longrightarrow \langle S[l \mapsto (d_1, \textsf{true})]; d_1 \rangle}$$

E-FREEZE-SIMPLE
$$\frac{S(l) = (d_1, frz_1)}{\langle S; \texttt{freeze} \ l \rangle \longrightarrow \langle S[l \mapsto (d_1, \textsf{true})]; d_1 \rangle}$$

Figure 3: An operational semantics for LVish.

LVish uses a reduction semantics based on evaluation contexts. The E-EVAL-CTXT rule is a standard context rule, allowing us to apply reductions within a context. The choice of context determines where evaluation can occur; in LVish, the order of evaluation is nondeterministic (that is, a given expression can generally reduce in various ways), 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 LVish, the arguments to `get`, `put`, `freeze`, and application expressions are *implicitly* evaluated concurrently.[4]

Arguments must be fully evaluated, however, before function application (β-reduction, modeled by the E-BETA rule) can occur. We can exploit this property to define `let par` as syntactic sugar:

$$\texttt{let par} \ x = e_1; \ y = e_2 \ \texttt{in} \ e_3 \ \triangleq \ ((\lambda x. \, (\lambda y. \, e_3)) \, e_1) \, e_2$$

Because we do not reduce under λ-terms, we can sequentially compose e_1 before e_2 by writing `let _ = e₁ in e₂`, which desugars to $(\lambda_-. \, e_2) \, e_1$. Sequential composition is useful, for instance, when allocating a new LVar before beginning a set of side-effecting `put`/`get`/`freeze` operations on it.

4.5 Semantics of **new**, **put**, and **get**

In LVish, the `new`, `put`, and `get` operations respectively create, write to, and read from LVars in the store:

- `new` (implemented by the E-NEW rule) extends the store with a binding for a new LVar whose initial state is $(\bot, \textsf{false})$, and returns the location l of that LVar (*i.e.*, a pointer to the LVar).

---

[4]This is in contrast to the original LVars formalism given in [20], which models parallelism with explicitly simultaneous reductions.

- `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.[5]

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 `put`s 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, because $p_1 \sqcup_p p_2 = \top_p$, but in the meantime, `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 answer of the program, which is guaranteed to subsequently fault.

4.6 The `freeze` − `after` − `with` Primitive

The LVish calculus includes a simple form of `freeze` that immediately freezes an LVar (see E-Freeze-Simple). More interesting is the `freeze` − `after` − `with` primitive, which models the "freeze-after" pattern described in Section 3.3. The expression `freeze` e_{lv} `after` e_{events} `with` e_{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`).

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

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

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 $\{e, \ldots\}$ 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 our use of evaluation contexts, any running callback can execute at any time, as if each is running in its own thread.

---

[5] We stress that, although $incomp(P)$ is given as a premise of the E-Get reduction rule (suggesting that it is checked at runtime), in our real implementation threshold sets are not written explicitly, and it is the data structure author's responsibility to ensure that any provided read operations have threshold semantics; see Section 6.

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, raising **error** by way of the E-PUT-ERR rule.

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 freeze − after − 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. Our implementation provides a special runParThenFreeze function that does so, and thereby guarantees full determinism.

4.7 Modeling Lattice Parameterization in Redex

We have developed a runnable version of the LVish calculus[6] using the PLT Redex semantics engineering toolkit [15]. In the Redex of today, it is not possible to directly parameterize a language definition by a lattice.[7] 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 3, 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)
```

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.

---

[6]Available at http://github.com/iu-parfunc/lvars.

[7]See discussion at http://lists.racket-lang.org/users/archive/2013-April/057075.html.

5   Quasi-Determinism for LVish

Our proof of quasi-determinism for LVish formalizes the claim we make in Section 1: that, for a given program, although some executions may raise exceptions, all executions that produce a final result will produce the same final result.

In this section, we give the statements of the main quasi-determinism theorem and the two most important supporting lemmas. The statements of the remaining lemmas, and proofs of all our theorems and lemmas, are included in Appendix B.

5.1   Quasi-Determinism and Quasi-Confluence

Our main result, Theorem 1, 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 1 (Quasi-Determinism). *If $\sigma \hookrightarrow^* \sigma'$ and $\sigma \hookrightarrow^* \sigma''$, and neither σ' nor σ'' can take a step, then either:*

1. *$\sigma' = \sigma''$ up to a permutation on locations π, or*

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

Theorem 1 follows from a series of *quasi-confluence* lemmas. The most important of these, Strong Local Quasi-Confluence (Lemma 2), says that if a configuration steps to two different configurations, then either there exists a single third configuration to which they both step (in at most one step), or one of them steps to **error**. Additional lemmas generalize Lemma 2's result to multiple steps by induction on the number of steps, eventually building up to Theorem 1.

Lemma 2 (Strong Local Quasi-Confluence). *If $\sigma \equiv \langle S;\ e \rangle \hookrightarrow \sigma_a$ and $\sigma \hookrightarrow \sigma_b$, then either:*

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

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

5.2   Independence

In order to show Lemma 2, we need a "frame property" for LVish that captures the idea that independent effects commute with each other. Lemma 3, the Independence lemma, establishes this property. Consider an expression e that runs starting in store S and steps to e', updating the store to S'. The Independence lemma allows us to make a double-edged guarantee about what will happen if we run e starting from a larger store $S \sqcup_S S''$: first, it will update the store to $S' \sqcup_S S''$; second, it 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 3 (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 $\langle S;\ e \rangle \hookrightarrow \langle S';\ e' \rangle$,*

- *$S' \sqcup_S S'' =_{frz} S$, and*

- *$S' \sqcup_S S'' \neq \top_S$.*

Lemma 3 requires as a 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. Finally, 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 4. Two stores S and S' are *equal in status* (written $S =_{frz} S'$) iff for all $l \in (dom(S) \cap dom(S'))$, if $S(l) = (d, frz)$ and $S'(l) = (d', frz')$, then $frz = frz'$.

Definition 5. A store S'' is *non-conflicting* with the transition $\langle S; e \rangle \longrightarrow \langle S'; e' \rangle$ iff $(dom(S') - dom(S)) \cap dom(S'') = \emptyset$.

6 Implementation

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

<div align="center">

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

</div>

Our library adopts the basic approach of the `Par` monad [24], 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 3 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:[8]

```
Par :: Determinism → * → *
```

together with the following suite of `run` functions:

```
runPar    :: Par Det a → a
runParIO :: Par lvl a → IO a
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.[9]

6.1 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.

---

[8]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`.

[9]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 [18]. 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 [2]. And in any case, monotonic data structures are usually much simpler to represent and implement than general ones.

6.2 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 `put`s to atoms, `get`s 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 `put`s and `get`s/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 [25]: 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 [11]). But idempotence also helps us deal with races between `put` and `get`/`addHandler`, as we explain below.

6.3 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.[10] 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.[11] 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 ()
```

---

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

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

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.

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.

6.4   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 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 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.

```haskell
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
    case curStat of
      Frozen → error "Attempt_to_change_a_frozen_LVar"
      Active listeners → B.foreach listeners $
        λ(Listener onUpd _) tok → onUpd d tok q
  k () q

freezeLV :: LVar a d → Par QuasiDet ()
freezeLV (LVar {status}) = mkPar $ λk q → do
  Sched.awaitClear q
  oldStat ← atomicModifyIORef status $ λs→(Frozen, s)
  case oldStat of
    Frozen → return ()
    Active listeners → B.foreach listeners $
      λ(Listener _ onFrz) tok → onFrz tok q
  k () q
```

Figure 4: Implementation of key lattice-generic functions.

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.[12]

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 `get`ting 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 `put`s that *caused* the freeze to take place check the frozen status *before* the freeze takes place; additional `put`s 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.

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.[13] 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 ::
```

---

[12]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 [16].

[13]One can use a high-performance *scalable non-zero indicator* [14] to implement `Counter`, but we have not yet done so.

```
  Maybe HandlerPool              -- Pool to enroll in
→ LVar a d                       -- LVar to listen to
→ (a → IO (Maybe (Par lvl ())))  -- Global callback
→ (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.[14]

7 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 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 Appendix C), we also give benchmarking results for LVish implementations of two graph-algorithm microbenchmarks: breadth-first search and maximal independent set.

7.1 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 [26].[15] 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:

---

[14]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.

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

```
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)
```

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 [23]. 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 todo)`. 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 `Set`s in the implementation serve a memoization purpose: they prevent repeated computations as we traverse the graph of states.

7.2   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 1! 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,
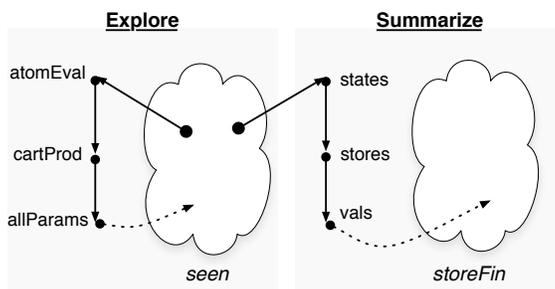
Figure 5: Simplified handler network for k-CFA. Exploration and summarization processes are driven by the same LVar. The triply-nested `forEach` calls in `summarize` become a chain of three handlers.

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 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 6 shows performance data for the "blur" benchmark drawn from a recent paper on k-CFA [13]. (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 6 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).
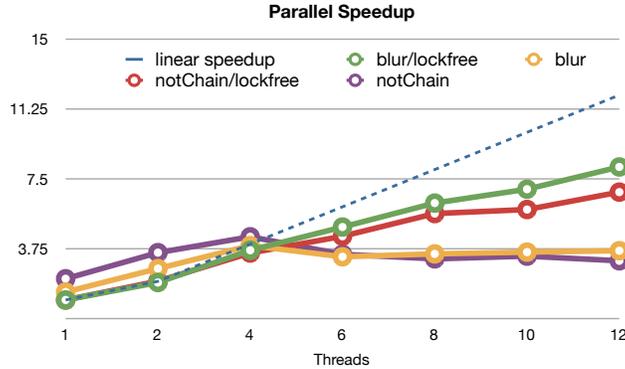
Parallel Speedup

Figure 6: 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.

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 [18].[16] 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.[17] 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.

8 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) [19], as well as in the more restricted *synchronous data flow* systems [21], 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 [17].

- In parallel *single-assignment languages* [32], "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* [1]— have appeared in Concurrent ML as `SyncVar`s [30]; in the Intel Concurrent Collections system [8]; in languages and libraries for high-performance computing, such as Chapel [10] and the Qthreads library [33]; and have even been implemented in hardware in Cray MTA machines [3]. Although most of these uses incorporate IVars

---

[16]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.

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

into already-nondeterministic programming environments, Haskell's `Par` monad [24]—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 2. Hence LVars provide a framework for generalizing and unifying these two existing approaches to deterministic parallelism.

Deterministic Parallel Java (DPJ)   DPJ [6, 5] 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.* [7] 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.* [29] 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) [22] 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 [9] 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) [31] 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 [12] 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.

Acknowledgments

References

[1] Arvind, Rishiyur S. Nikhil, and Keshav K. Pingali. I-structures: data structures for parallel computing. *ACM Trans. Program. Lang. Syst.*, 11, October 1989.

[2] Hagit Attiya, Rachid Guerraoui, Danny Hendler, Petr Kuznetsov, Maged M. Michael, and Martin Vechev. Laws of order: expensive synchronization in concurrent algorithms cannot be eliminated. In *POPL*, 2011.

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

[4] Guy E. Blelloch, Jeremy T. Fineman, Phillip B. Gibbons, and Julian Shun. Internally deterministic parallel algorithms can be fast. In *PPoPP*, 2012.

[5] Robert L. Bocchino, Jr., Vikram S. Adve, Sarita V. Adve, and Marc Snir. Parallel programming must be deterministic by default. In *HotPar*, 2009.

[6] Robert L. Bocchino, Jr., Vikram S. Adve, Danny Dig, Sarita V. Adve, Stephen Heumann, Rakesh Komuravelli, Jeffrey Overbey, Patrick Simmons, Hyojin Sung, and Mohsen Vakilian. A type and effect system for deterministic parallel Java. In *OOPSLA*, 2009.

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

[8] Zoran Budimlić, Michael Burke, Vincent Cavé, Kathleen Knobe, Geoff Lowney, Ryan Newton, Jens Palsberg, David Peixotto, Vivek Sarkar, Frank Schlimbach, and Sağnak Taşirlar. Concurrent Collections. *Sci. Program.*, 18, August 2010.

[9] Sebastian Burckhardt and Daan Leijen. Semantics of concurrent revisions. In *ESOP*, 2011.

[10] 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.

[11] David Chase and Yossi Lev. Dynamic circular work-stealing deque. In *SPAA*, 2005.

[12] Neil Conway, William Marczak, Peter Alvaro, Joseph M. Hellerstein, and David Maier. Logic and lattices for distributed programming. In *SOCC*, 2012.

[13] Christopher Earl, Ilya Sergey, Matthew Might, and David Van Horn. Introspective pushdown analysis of higher-order programs. In *ICFP*, 2012.

[14] Faith Ellen, Yossi Lev, Victor Luchangco, and Mark Moir. SNZI: Scalable NonZero Indicators. In *PODC*, 2007.

[15] Matthias Felleisen, Robert Bruce Findler, and Matthew Flatt. *Semantics Engineering with PLT Redex*. The MIT Press, 1st edition, 2009.

[16] Keir Fraser. *Practical lock-freedom*. PhD thesis, 2004.

[17] Michael I. Gordon, William Thies, Michal Karczmarek, Jasper Lin, Ali S. Meli, Christopher Leger, Andrew A. Lamb, Jeremy Wong, Henry Hoffman, David Z. Maze, and Saman Amarasinghe. A stream compiler for communication-exposed architectures. In *ASPLOS*, 2002.

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

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

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

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

[22] Daan Leijen, Manuel Fahndrich, and Sebastian Burckhardt. Prettier concurrency: purely functional concurrent revisions. In *Haskell*, 2011.

[23] Simon Marlow, Patrick Maier, Hans-Wolfgang Loidl, Mustafa K. Aswad, and Phil Trinder. Seq no more: better strategies for parallel Haskell. In *Haskell*, 2010.

[24] Simon Marlow, Ryan Newton, and Simon Peyton Jones. A monad for deterministic parallelism. In *Haskell*, 2011.

[25] Maged M. Michael, Martin T. Vechev, and Vijay A. Saraswat. Idempotent work stealing. In *PPoPP*, 2009.

[26] Matthew 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/.

[27] Rishiyur S. Nikhil. Id language reference manual, 1991.

[28] Simon L. Peyton Jones, Roman Leshchinskiy, Gabriele Keller, and Manuel M. T. Chakravarty. Harnessing the multicores: Nested data parallelism in Haskell. In *FSTTCS*, 2008.

[29] Aleksandar Prokopec, Heather Miller, Tobias Schlatter, Philipp Haller, and Martin Odersky. FlowPools: a lock-free deterministic concurrent dataflow abstraction. In *LCPC*, 2012.

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

[31] Marc Shapiro, Nuno Preguiça, Carlos Baquero, and Marek Zawirski. Conflict-free replicated data types. In *SSS*, 2011.

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

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

A   Soundness of Freezing

In this appendix, we show that adding "status bits" to an application-specific lattice preserves its algebraic structure.

Remark 1 (Lattice terminology). Throughout this section, we use "lattice" as shorthand for "bounded join-semilattice with a designated greatest element". In particular, when we speak of a "lattice $(D, \sqsubseteq, \bot, \top)$", we are referring to a bounded join-semilattice with elements D, ordered by $\sqsubseteq$, with $\bot$ as the least element, and with a designated greatest element $\top$.

Lemma 4 (Partition of D_p). *Suppose $(D, \sqsubseteq, \bot, \top)$ is a lattice, and that $(D_p, \sqsubseteq_p, \bot_p, \top_p) = \mathrm{Freeze}(D, \sqsubseteq, \bot, \top)$, 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 1. □

Definition 6. We define a binary operator $\sqcup_p \in D_p \times D_p \to D_p$ as follows:

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

Lemma 5 (Lattice structure). *(This lemma is a more detailed version of Lemma 1 from the main text of the paper.) Suppose that $(D, \sqsubseteq, \bot, \top)$ is a lattice, and that $(D_p, \sqsubseteq_p, \bot_p, \top_p) = \mathrm{Freeze}(D, \sqsubseteq, \bot, \top)$. 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.

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 4, either $v = (d, \mathsf{false})$ with $d \in D$, or $v = (x, \mathsf{true})$ with $x \in X$, where $X = D - \{\top\}$.
      - Suppose $v = (d, \mathsf{false})$:
         By the reflexivity of $\sqsubseteq$, we know $d \sqsubseteq d$.
         By the definition of $\sqsubseteq_p$, we know $(d, \mathsf{false}) \sqsubseteq_p (d, \mathsf{false})$.
      - Suppose $v = (x, \mathsf{true})$:
         By the reflexivity of equality, $x = x$.
         By the definition of $\sqsubseteq_p$, we know $(x, \mathsf{true}) \sqsubseteq_p (x, \mathsf{true})$.

(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 $v_1 = (d_1, \mathsf{false})$ and $v_2 = (d_2, \mathsf{false})$ and $v_3 = (d_3, \mathsf{false})$:
  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 $(d_1, \mathsf{false}) \sqsubseteq_p (d_3, \mathsf{false})$.
  Hence $v_1 \sqsubseteq_p v_3$.

- Case $v_1 = (d_1, \mathsf{false})$ and $v_2 = (d_2, \mathsf{false})$ and $v_3 = (x_3, \mathsf{true})$:
  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 $(d_1, \mathsf{false}) \sqsubseteq_p (x_3, \mathsf{true})$.
  Hence $v_1 \sqsubseteq_p v_3$.

- Case $v_1 = (d_1, \mathsf{false})$ and $v_2 = (x_2, \mathsf{true})$ and $v_3 = (d_3, \mathsf{false})$:
  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 $(d_1, \mathsf{false}) \sqsubseteq_p (d_3, \mathsf{false})$.
  Hence $v_1 \sqsubseteq_p v_3$.

- Case $v_1 = (d_1, \mathsf{false})$ and $v_2 = (x_2, \mathsf{true})$ and $v_3 = (x_3, \mathsf{true})$:
  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 $(d_1, \mathsf{false}) \sqsubseteq_p (x_3, \mathsf{true})$.
  Hence $v_1 \sqsubseteq_p v_3$.

- Case $v_1 = (x_1, \mathsf{true})$ and $v_2 = (d_2, \mathsf{false})$ and $v_3 = (d_3, \mathsf{false})$:
  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 $(x_1, \mathsf{true}) \sqsubseteq_p (d_3, \mathsf{false})$.
  Hence $v_1 \sqsubseteq_p v_3$.

- Case $v_1 = (x_1, \mathsf{true})$ and $v_2 = (d_2, \mathsf{false})$ and $v_3 = (x_3, \mathsf{true})$:
  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 $v_1 = (x_1, \mathsf{true})$ and $v_2 = (x_2, \mathsf{true})$ and $v_3 = (d_3, \mathsf{false})$:
  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 $(x_1, \mathsf{true}) \sqsubseteq_p (d_3, \mathsf{false})$.
  Hence $v_1 \sqsubseteq_p v_3$.

- Case $v_1 = (x_1, \mathsf{true})$ and $v_2 = (x_2, \mathsf{true})$ and $v_3 = (x_3, \mathsf{true})$:
  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 $(x_1, \mathsf{true}) \sqsubseteq_p (x_3, \mathsf{true})$.
  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 $v_1 = (d_1, \mathsf{false})$ and $v_2 = (d_2, \mathsf{false})$:
  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 $v_1 = (d_1, \mathsf{false})$ and $v_2 = (x_2, \mathsf{true})$:
  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 $v_1 = (x_1, \mathsf{true})$ and $v_2 = (d_2, \mathsf{false})$:
  Similar to the previous case.

- Case $v_1 = (x_1, \mathsf{true})$ and $v_2 = (x_2, \mathsf{true})$:
  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 6 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 $v_1 = (d_1, \mathsf{false})$ and $v_2 = (d_2, \mathsf{false})$.
  Now case on v:

  – Case $v = (d, \mathsf{false})$:
    By the definition of $\sqcup_p$, $(d_1, \mathsf{false}) \sqcup_p (d_2, \mathsf{false}) = (d_1 \sqcup d_2, \mathsf{false})$.
    By inversion on $(d_1, \mathsf{false}) \sqsubseteq_p (d, \mathsf{false})$, $d_1 \sqsubseteq l$.
    By inversion on $(d_2, \mathsf{false}) \sqsubseteq_p (d, \mathsf{false})$, $d_2 \sqsubseteq l$.
    Hence l is an upper bound for d_1 and d_2.
    Hence $d_1 \sqcup d_2 \sqsubseteq l$.
    Hence $(d_1 \sqcup d_2, \mathsf{false}) \sqsubseteq_p (d, \mathsf{false})$.
    Hence $v_1 \sqcup_p v_2 \sqsubseteq_p v$.

  – Case $v = (x, \mathsf{true})$:
    By the definition of $\sqcup_p$, $(d_1, \mathsf{false}) \sqcup_p (d_2, \mathsf{false}) = (d_1 \sqcup d_2, \mathsf{false})$.
    By inversion on $(d_1, \mathsf{false}) \sqsubseteq_p (x, \mathsf{true})$, $d_1 \sqsubseteq x$.
    By inversion on $(d_2, \mathsf{false}) \sqsubseteq_p (x, \mathsf{true})$, $d_2 \sqsubseteq x$.
    Hence x is an upper bound for d_1 and d_2.
    Hence $d_1 \sqcup d_2 \sqsubseteq x$.
    Hence $(d_1 \sqcup d_2, \mathsf{false}) \sqsubseteq_p (x, \mathsf{true})$.
    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 $(d_1, \mathsf{false}) \sqcup_p (x_2, \mathsf{true}) = (x_2, \mathsf{true})$.

  By the definition of $\sqcup_p$, we know $(d_1, \mathsf{false}) \sqsubseteq_p (x_2, \mathsf{true})$.

  Hence $v_1 \sqsubseteq_p v_1 \sqcup_p v_2$.

  By reflexivity, $(x_2, \mathsf{true}) \sqsubseteq_p (x_2, \mathsf{true})$.

  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 $(d_1, \mathsf{false}) \sqcup_p (x_2, \mathsf{true}) = (\top, \mathsf{false})$.

  Since $d_1 \sqsubseteq \top$, by the definition of $\sqsubseteq_p$ we know $(d_1, \mathsf{false}) \sqsubseteq (\top, \mathsf{false})$.

  Hence $v_1 \sqsubseteq_p v_1 \sqcup_p v_2$.

  By the definition of $\sqsubseteq_p$, we know $(x_2, \mathsf{true}) \sqsubseteq (\top, \mathsf{false})$.

  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 $v_1 = (x_1, \mathsf{true})$ and $v_2 = (d_2, \mathsf{false})$:

  Symmetric with the previous case.

- Case $v_1 = (x_1, \mathsf{true})$ and $v_2 = (x_2, \mathsf{true})$:

  Consider whether x_1 equals x_2.

  - Case $x_1 = x_2$:

    By the definition $\sqcup_p$, $(x_1, \mathsf{true}) \sqcup_p (x_2, \mathsf{true}) = (x_1, \mathsf{true})$.

    By reflexivity, $(x_1, \mathsf{true}) \sqsubseteq_p (x_1, \mathsf{true})$.

    Hence $v_1 \sqsubseteq_p v_1 \sqcup_p v_2$.

    By reflexivity, $(x_2, \mathsf{true}) \sqsubseteq_p (x_1, \mathsf{true})$.

    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 $\sqcup_p$, $(x_1, \mathsf{true}) \sqcup_p (x_2, \mathsf{true}) = (\top, \mathsf{false})$.

    By the definition of $\sqsubseteq_p$, $(x_1, \mathsf{true}) \sqsubseteq_p (\top, \mathsf{false})$.

    Hence $v_1 \sqsubseteq_p v_1 \sqcup_p v_2$.

    By the definition of $\sqsubseteq_p$, $(x_2, \mathsf{true}) \sqsubseteq_p (\top, \mathsf{false})$.

    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. $\bot_p$ is the least element of D_p.

   $\bot_p$ is defined to be $(\bot, \mathsf{false})$. 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 4, 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 $\sqsubseteq_p$, $(\bot, \mathsf{false}) \sqsubseteq_p (d, \mathsf{false})$ iff $\bot \sqsubseteq d$.

     Since $\bot$ is the least element of D, $\bot \sqsubseteq d$.

     Therefore $\bot_p = (\bot, \mathsf{false}) \sqsubseteq_p (d, \mathsf{false})$.

   - (x, true) for all $x \in X$:

     By the definition of $\sqsubseteq_p$, $(\bot, \mathsf{false}) \sqsubseteq_p (x, \mathsf{true})$ iff $\bot \sqsubseteq x$.

     Since $\bot$ is the least element of D, $\bot \sqsubseteq x$.

     Therefore $\bot_p = (\bot, \mathsf{false}) \sqsubseteq_p (x, \mathsf{true})$.

   Therefore $\bot_p$ 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 $(\top, \mathsf{false})$. 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 4, 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 $\sqsubseteq_p$, $(d, \mathsf{false}) \sqsubseteq_p (\top, \mathsf{false})$ iff $d \sqsubseteq \top$.
     Since $\top$ is the greatest element of D, $d \sqsubseteq \top$.
     Therefore $(d, \mathsf{false}) \sqsubseteq_p (\top, \mathsf{false}) = \top_p$.
   - (x, true) for all $x \in X$:
     By the definition of $\sqsubseteq_p$, $(x, \mathsf{true}) \sqsubseteq_p (\top, \mathsf{false})$ iff $\top \sqsubseteq \top$.
     Therefore $(x, \mathsf{true}) \sqsubseteq_p (\top, \mathsf{false}) = \top_p$.

   Therefore all elements of D_p are less than or equal to $\top_p$.

$\square$

B Quasi-determinism for LVish

In this appendix, we show that LVish programs are quasi-deterministic: on every run, a given LVish program will either produce the same answer or raise an error.

For working with stores, we make use of Definitions 2, 3, 4, and 5 from the main text of the paper, as well as the following definition:

Definition 7. 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 $l \in dom(S_1) \cap dom(S_2)$ 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:
  - $dom(S) = dom(S_1) \cup dom(S_2)$, and
  - For all $l \in dom(S)$:

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

B.1 Decomposition Preservation

Lemma 6 pertains to situations where an LVish expression e can be decomposed two ways: into a context E_0 and a redex e_0, and into a context E_1 and a redex e_1, where E_0 and E_1 differ.

It says that, if $E_0[e_0]$ and $E_1[e_1]$ are initially equivalent (to each other and to e), then, if we substitute any other e_0' for e_0, resulting in $E_0[e_0']$, there will be some context E_1' that we can substitute for E_1 in $E_1[e_1']$, resulting in an expression $E_1'[e_1]$ that is equivalent to $E_0[e_0']$.

Lemma 6 (Decomposition Preservation). *Suppose $e = E_0[e_0]$ and $e = E_1[e_1]$, where E_0 and E_1 are distinct evaluation contexts and e_0 and e_1 are redexes. Then, for all e_0', there exists an evaluation context E_1' such that $E_0[e_0'] = E_1'[e_1]$.*

Proof. Consider arbitrary e_0'. The proof proceeds by induction on the structure of e.

- Case $e = x$:

  Since there is no decomposition of x into a context and a redex, this case cannot occur. (The only applicable context is $[\ ]$, and x is not a redex.)

- Case $e = v$:

  Since there is no decomposition of v into a context and a redex, this case cannot occur. (The only applicable context is $[\ ]$, and values are not redexes.)

- Case $e = e_a\ e_b$:

  First, note that e cannot be a reducible expression. If that were the case, then we would have $e_a = \lambda x.\,e'_a$ for some e'_a and $e_b = v$ for some value v. Since $\lambda x.\,e'_a$ and v are both values, then there would be only one decomposition of e into context and redex (context $[\ ]$ and redex e), which contradicts the lemma's assumption that e decomposes into $E_0[e_0]$ and $E_1[e_1]$, where E_0 and E_1 are distinct.

  Now, let us proceed by case analysis on E_0 and E_1. Note that the number of cases we have to consider is limited by the fact that $e = e_a\ e_b$ is an application.

    - Case $E_0 = e_a\ E_{b_0}$ and $E_1 = e_a\ E_{b_1}$:
      We have that $e = E_0[e_0]$ and $e = E_1[e_1]$ and $e = e_a\ e_b$.
      Hence $e = E_0[e_0] = e_a\ E_{b_0}[e_0] = E_1[e_1] = e_a\ E_{b_1}[e_1]$.
      Hence $e_b = E_{b_0}[e_0] = E_{b_1}[e_1]$.
      Note that E_{b_0} and E_{b_1} must be distinct, since E_0 and E_1 are distinct by assumption, and $E_0 = e_a\ E_{b_0}$ and $E_1 = e_a\ E_{b_1}$.
      Also, note that e_0 and e_1 are redexes, by assumption.
      Hence, by IH, there exists an E'_{b_1} such that $E_{b_0}[e'_0] = E'_{b_1}[e_1]$.
      Hence $e_a\ E_{b_0}[e'_0] = e_a\ E'_{b_1}[e_1]$.
      Choose $E'_1 = e_a\ E'_{b_1}$.
      Then $E_0[e'_0] = E'_1[e_1]$.
    - Case $E_0 = E_{a_0}\ e_b$ and $E_1 = E_{a_1}\ e_b$:
      Similar to the previous case.
    - Case $E_0 = e_a\ E_{b_0}$ and $E_1 = E_{a_1}\ e_b$:
      We have that $e = E_0[e_0]$ and $e = E_1[e_1]$ and $e = e_a\ e_b$.
      Hence $e = e_a\ E_{b_0}[e_0] = E_{a_1}[e_1]\ e_b = e_a\ e_b$.
      Hence $e_a = E_{a_1}[e_1]$ and $e_b = E_{b_0}[e_0]$.
      Choose $E'_1 = E_{a_1}\ E_{b_0}[e'_0]$.
      Then $E_0[e'_0] = e_a\ E_{b_0}[e'_0] = E_{a_1}[e_1]\ E_{b_0}[e'_0] = E'_1[e_1]$.
    - Case $E_0 = E_{a_0}\ e_b$ and $E_1 = E_a\ E_{b_1}$:
      Similar to the previous case.

- Case $e = \texttt{get}\ e_a\ e_b$:

  Similar to the application case.

- Case $e = \texttt{put}\ e_a\ e_b$:

  Similar to the application case.

- Case $e = \texttt{freeze}\ e_a$:

  In this case, $E_0 = \texttt{freeze}\ E_{a_0}$ and $E_1 = \texttt{freeze}\ E_{a_1}$.
  So $e' = E_{a_0}[e_0] = E_{a_1}[e_1]$.

Note that E_{a_0} and E_{a_1} are distinct, since, if they were not, then E_0 and E_1 would also not be distinct, contradicting the assumption of the theorem.

Hence by IH, there exists an E'_{a_1} such that $E_{a_0}[e'_0] = E'_{a_1}[e_1]$.

Hence, by congruence of equality, $\texttt{freeze}\ E_{a_0}[e'_0] = \texttt{freeze}\ E'_{a_1}[e_1]$.

So we can take $E'_1 = \texttt{freeze}\ E'_{a_1}$.

- Case $e = \texttt{freeze}\ e_a\ \texttt{after}\ e_b\ \texttt{with}\ e_c$:

  This is a reducible expression, and hence $E_0 = E_1 = [\,]$ and $e_0 = e_1 = e$, which contradicts the hypothesis.

- Case $e = \texttt{freeze}\ v_a\ \texttt{after}\ v_b\ \texttt{with}\ v_c, \{e_1, \ldots, e_n\}, H$:

  First, note that e cannot be a reducible expression (*i.e.*, each $e_i = v_i$ for 1 to n). If that were the case, then $E_0 = E_1 = [\,]$, which contradicts the assumption of the theorem.

  Therefore $E_0 = \texttt{freeze}\ v_a\ \texttt{after}\ v_b\ \texttt{with}\ v_c, \{v_1, \ldots, E_{v_i}, \ldots, v_n\}, H$.
  Therefore $E_1 = \texttt{freeze}\ v_a\ \texttt{after}\ v_b\ \texttt{with}\ v_c, \{v_1, \ldots, E_{v_j}, \ldots, v_n\}, H$.
  Now consider whether $i = j$.

  - Case $i = j$:

    In this case, we know that $E_{v_i}[e_0] = E_{v_j}[e_1]$.
    By induction, we have E'_{v_j} such that $E_{v_i}[e'_0] = E'_{v_j}[e_1]$.

    Then we can take $E'_1 = \texttt{freeze}\ v_a\ \texttt{after}\ v_b\ \texttt{with}\ v_c, \left\{e_1, \ldots, E'_{v_j}, \ldots, e_n\right\}, H$.

  - Case $i \neq j$:

    Without loss of generality, suppose $i < j$.
    In this case, we know that $e_i = E_{v_i}[e_0]$ and $e_j = E_{v_j}[e_1]$.
    Choose $E'_1 = \texttt{freeze}\ v_a\ \texttt{after}\ v_b\ \texttt{with}\ v_c, \{\ldots, E_{v_i}[e'_0], \ldots, E_{v_j}, \ldots\}, H$.
    Then $E'_0[e'_0] = \texttt{freeze}\ v_a\ \texttt{after}\ v_b\ \texttt{with}\ v_c, \{\ldots, E_{v_i}[e'_0], \ldots, v_j, \ldots\}, H$.
    So $E'_0[e'_0] = \texttt{freeze}\ v_a\ \texttt{after}\ v_b\ \texttt{with}\ v_c, \{\ldots, E_{v_i}[e'_0], \ldots, E_{v_j}[e_1], \ldots\}, H = E'_1[e_1]$.

$\square$

B.2 Monotonicity

Lemma 7 (Monotonicity). *If $\langle S;\ e \rangle \longleftrightarrow \langle S';\ e' \rangle$, then $S \sqsubseteq_S S'$.*

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

- Case E-EVAL-CTXT:

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

  To show: $S \sqsubseteq_S S'$.

  From the premise of E-EVAL-CTXT, $\langle S;\ e \rangle \longleftrightarrow \langle S';\ e' \rangle$.

  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: $\langle S;\ \texttt{new} \rangle \longleftrightarrow \langle S[l \mapsto (\bot, \textsf{false})];\ l \rangle$.

  To show: $S \sqsubseteq_S S[l \mapsto (\bot, \textsf{false})]$.

  By Definition 3, we have to show that $dom(S) \subseteq dom(S[l \mapsto (\bot, \textsf{false})])$ and that for all $l' \in dom(S)$, $S(l') \sqsubseteq_p (S[l \mapsto (\bot, \textsf{false})])(l')$.

By the definition of store update, $S[l \mapsto (d_1, \mathsf{true})]$ can only either update an existing binding in S or extend S with a new binding.

Hence $dom(S) \subseteq dom(S[l \mapsto (\bot, \mathsf{false})])$.

From the side condition of E-NEW, $l \notin dom(S)$.

Hence $S[l \mapsto (\bot, \mathsf{false})]$ adds a new binding for l in S.

Hence $S[l \mapsto (d_1, \mathsf{true})]$ does not update any existing bindings in S.

Hence, for all $l' \in dom(S), S(l') \sqsubseteq_p (S[l \mapsto (d_1, \mathsf{true})])(l')$.

Therefore $S \sqsubseteq_S S[l \mapsto (\bot, \mathsf{false})]$, as required.

- Case E-PUT:

  Given: $\langle S; \texttt{put } l\ d_2 \rangle \longrightarrow \langle S[l \mapsto p_2]; \texttt{( )} \rangle$.

  To show: $S \sqsubseteq_S S[l \mapsto p_2]$.

  By Definition 3, 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, $p_2 = p_1 \sqcup_p (d_2, \mathsf{false})$.

  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: $\langle S; \texttt{put } l\ d_2 \rangle \longrightarrow \mathbf{error}$.

  By the definition of $\mathbf{error}$, $\mathbf{error} = \langle \top_S; e \rangle$ 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: $\langle S; \texttt{freeze } l \texttt{ after } Q \texttt{ with } v, \{v \ldots\}, H \rangle \longrightarrow \langle S[l \mapsto (d_1, \mathsf{true})]; d_1 \rangle$.

  To show: $S \sqsubseteq_S S[l \mapsto (d_1, \mathsf{true})]$.

  By Definition 3, we have to show that $dom(S) \subseteq dom(S[l \mapsto (d_1, \mathsf{true})])$ and that for all $l' \in dom(S)$, $S(l') \sqsubseteq_p (S[l \mapsto (d_1, \mathsf{true})])(l')$.

By the definition of store update, $S[l \mapsto (d_1, \mathsf{true})]$ can only either update an existing binding in S or extend S with a new binding.

Hence $dom(S) \subseteq dom(S[l \mapsto (d_1, \mathsf{true})])$.

From the premises of E-FREEZE-FINAL, $S(l) = (d_1, frz_1)$. Therefore $l \in dom(S)$.

Hence $S[l \mapsto (d_1, \mathsf{true})]$ updates the existing binding for l in S from (d_1, frz_1) to (d_1, true).

By the definition of $\sqsubseteq_p$, $(d_1, frz_1) \sqsubseteq_p (d_1, \mathsf{true})$.

$S[l \mapsto (d_1, \mathsf{true})]$ does not update any other bindings in S, hence, for all $l' \in dom(S)$, $S(l') \sqsubseteq_p (S[l \mapsto (d_1, \mathsf{true})])(l')$.

Hence $S \sqsubseteq_S S[l \mapsto (d_1, \mathsf{true})]$, as required.

- Case E-FREEZE-SIMPLE:

  Given: $\langle S;\ \texttt{freeze}\ l \rangle \longrightarrow \langle S[l \mapsto (d_1, \mathsf{true})];\ d_1 \rangle$.

  To show: $S \sqsubseteq_S S[l \mapsto (d_1, \mathsf{true})]$.

  Similar to the previous case.

$\square$

B.3 Independence

This is the proof of Lemma 3 from the main text of the paper.

Proof. Consider arbitrary S'' such that S'' is non-conflicting with $\langle S;\ e \rangle \longrightarrow \langle S';\ e' \rangle$ and $S' \sqcup_S S'' =_{frz} S$ and $S' \sqcup_S S'' \neq \top_S$.

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

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

   The assumption that $S' \sqcup_S S'' =_{frz} S$ is only needed in the E-FREEZE-FINAL and E-FREEZE-SIMPLE cases.

- Case E-EVAL-CTXT:

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

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

  From the premise of E-EVAL-CTXT, we have that $\langle S;\ e \rangle \longrightarrow \langle S';\ e' \rangle$.

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

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

- Case E-BETA:

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

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

  Immediate by E-BETA.

- Case E-NEW:

  Given: $\langle S;\ \texttt{new} \rangle \longrightarrow \langle S[l \mapsto (\bot, \mathsf{false})];\ l \rangle$.

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

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

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

Therefore $l \notin dom(S'')$.

From the side condition of E-NEW, $l \notin dom(S)$.

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

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

Therefore $\langle S \sqcup_S S''; \mathtt{new} \rangle \longleftrightarrow \langle (S \sqcup_S S'')[l \mapsto (\bot, \mathsf{false})]; l \rangle$.

Note that:

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

Therefore $\langle S \sqcup_S S''; \mathtt{new} \rangle \longleftrightarrow \langle S[l \mapsto (\bot, \mathsf{false})] \sqcup_S S''; l \rangle$, as we were required to show.

- Case E-PUT:

  Given: $\langle S; \mathtt{put}\ l\ d_2 \rangle \longleftrightarrow \langle S[l \mapsto p_2]; \mathtt{()} \rangle$.

  To show: $\langle S \sqcup_S S''; \mathtt{put}\ l\ d_2 \rangle \longleftrightarrow \langle S[l \mapsto p_2] \sqcup_S S''; \mathtt{()} \rangle$.

  We will first show that

  $\langle S \sqcup_S S''; \mathtt{put}\ l\ d_2 \rangle \longleftrightarrow \langle (S \sqcup_S S'')[l \mapsto p_2]; \mathtt{()} \rangle$

  and then show why this is sufficient.

  We proceed by cases on l:

  - $l \notin dom(S'')$:
    By assumption, $S[l \mapsto p_2] \sqcup_S S'' \neq \top_S$.
    By Lemma 7, $S \sqsubseteq_S S[l \mapsto p_2]$.
    Hence $S \sqcup_S S'' \neq \top_S$.
    Therefore, by Definition 7, $(S \sqcup_S S'')(l) = S(l)$.
    From the premises of E-PUT, $S(l) = p_1$.
    Hence $(S \sqcup_S S'')(l) = p_1$.
    From the premises of E-PUT, $p_2 = p_1 \sqcup_p (d_2, \mathsf{false})$ and $p_2 \neq \top_p$.
    Therefore, by E-PUT, we have: $\langle S \sqcup_S S''; \mathtt{put}\ l\ d_2 \rangle \longleftrightarrow \langle (S \sqcup_S S'')[l \mapsto p_2]; \mathtt{()} \rangle$.

  - $l \in dom(S'')$:
    By assumption, $S[l \mapsto p_2] \sqcup_S S'' \neq \top_S$.
    By Lemma 7, $S \sqsubseteq_S S[l \mapsto p_2]$.
    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, $p_2 = p_1 \sqcup_p (d_2, \mathsf{false})$.
    Let $p_2' = p_1' \sqcup_p (d_2, \mathsf{false})$.
    Hence $p_2 \sqsubseteq_p p_2'$.
    By assumption, $S[l \mapsto p_2] \sqcup_S S'' \neq \top_S$.
    Therefore, by Definition 7, $p_2 \sqcup_S S''(l) \neq \top_p$.

Note that:

$$\top_p \neq p_2 \sqcup_S S''(l)$$
$$= p_1 \sqcup_p (d_2, \mathsf{false}) \sqcup_p S''(l)$$
$$= S(l) \sqcup_p (d_2, \mathsf{false}) \sqcup_p S''(l)$$
$$= S(l) \sqcup_p S''(l) \sqcup_p (d_2, \mathsf{false})$$
$$= (S \sqcup_S S'')(l) \sqcup_p (d_2, \mathsf{false})$$
$$= p_1' \sqcup_p (d_2, \mathsf{false})$$
$$= p_2'.$$

Hence $p_2' \neq \top_p$.

Hence $(S \sqcup_S S'')(l) = p_1'$ and $p_2' = p_1' \sqcup_p (d_2, \mathsf{false})$ and $p_2' \neq \top_p$.

Therefore, by E-PUT we have: $\langle S \sqcup_S S''; \, \mathtt{put}\ l\ d_2 \rangle \longrightarrow \langle (S \sqcup_S S'')[l \mapsto p_2']; \, () \rangle$.

Note that:

$$((S \sqcup_S S'')[l \mapsto p_2'])(l) = (S \sqcup_S S'')(l) \sqcup_p ([l \mapsto p_2'])(l)$$
$$= p_1' \sqcup_p p_2'$$
$$= p_1' \sqcup_p p_1' \sqcup_p (d_2, \mathsf{false})$$
$$= p_1' \sqcup_p (d_2, \mathsf{false})$$

and

$$((S \sqcup_S S'')[l \mapsto p_2])(l) = (S \sqcup_S S'')(l) \sqcup_p ([l \mapsto p_2])(l)$$
$$= p_1' \sqcup_p p_2$$
$$= p_1' \sqcup_p p_1 \sqcup_p (d_2, \mathsf{false})$$
$$= p_1' \sqcup_p (d_2, \mathsf{false}) \qquad\qquad (\text{since } p_1 \sqsubseteq_p p_1').$$

Therefore $(S \sqcup_S S'')[l \mapsto p_2'] = (S \sqcup_S S'')[l \mapsto p_2]$.

Therefore, $\langle S \sqcup_S S''; \, \mathtt{put}\ l\ d_2 \rangle \longrightarrow \langle (S \sqcup_S S'')[l \mapsto p_2]; \, () \rangle$.

Note that:

$$(S \sqcup_S S'')[l \mapsto p_2] = S[l \mapsto p_2] \sqcup_S S''[l \mapsto p_2]$$
$$= S \sqcup_S [l \mapsto p_2] \sqcup_S S'' \sqcup_S [l \mapsto p_2]$$
$$= S \sqcup_S [l \mapsto p_2] \sqcup_S S''$$
$$= S[l \mapsto p_2] \sqcup_S S''.$$

Therefore $\langle S \sqcup_S S''; \, \mathtt{put}\ l\ d_2 \rangle \longrightarrow \langle S[l \mapsto p_2] \sqcup_S S''; \, () \rangle$, as we were required to show.

- Case E-GET:

  Given: $\langle S; \, \mathtt{get}\ l\ P \rangle \longrightarrow \langle S; \, p_2 \rangle$.

  To show: $\langle S \sqcup_S S''; \, \mathtt{get}\ l\ P \rangle \longrightarrow \langle S \sqcup_S S''; \, p_2 \rangle$.

  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 $\sqsubseteq_p$, $p_2 \sqsubseteq_p p_1'$.

37

Hence, $S(l) = p_1'$ and $incomp(P)$ and $p_2 \in P$ and $p_2 \sqsubseteq_p p_1'$.

Therefore, by E-GET,

$\langle S \sqcup_S S''; \text{ get } l\ P \rangle \longrightarrow \langle S \sqcup_S S''; p_2 \rangle$,

as we were required to show.

- Case E-FREEZE-INIT:

  Given: $\langle S; \text{ freeze } l \text{ after } Q \text{ with } \lambda x. e \rangle \longrightarrow$
  $\langle S; \text{ freeze } l \text{ after } Q \text{ with } \lambda x. e, \{\}, \{\} \rangle$.

  To show: $\langle S \sqcup_S S''; \text{ freeze } l \text{ after } Q \text{ with } \lambda x. e \rangle \longrightarrow$
  $\langle S \sqcup_S S''; \text{ freeze } l \text{ after } Q \text{ with } \lambda x. e, \{\}, \{\} \rangle$.

  Immediate by E-FREEZE-INIT.

- Case E-SPAWN-HANDLER:

  Given:

  $\langle S; \text{ freeze } l \text{ after } Q \text{ with } \lambda x. e_0, \{e, \dots\}, H \rangle \longrightarrow$
  $\langle S; \text{ freeze } l \text{ after } Q \text{ with } \lambda x. e_0, \{e_0[x := d_2], e, \dots\}, \{d_2\} \cup H \rangle$.

  To show:

  $\langle S \sqcup_S S''; \text{ freeze } l \text{ after } Q \text{ with } \lambda x. e_0, \{e, \dots\}, H \rangle \longrightarrow$
  $\langle S \sqcup_S S''; \text{ freeze } l \text{ after } Q \text{ with } \lambda x. e_0, \{e_0[x := d_2], e, \dots\}, \{d_2\} \cup H \rangle$.

  From the premises of E-SPAWN-HANDLER, $S(l) = (d_1, frz_1)$ 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 $(S \sqcup_S S'')(l) = (d_1', frz_1')$ where $(d_1, frz_1) \sqsubseteq_p (d_1', frz_1')$.

  By Definition 1, $d_1 \sqsubseteq d_1'$.

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

  Hence $(S \sqcup_S S'')(l) = (d_1', frz_1')$ and $d_2 \sqsubseteq d_1'$ and $d_2 \notin H$ and $d_2 \in Q$.

  Therefore, by E-SPAWN-HANDLER,

  $\langle S \sqcup_S S''; \text{ freeze } l \text{ after } Q \text{ with } \lambda x. e_0, \{e, \dots\}, H \rangle \longrightarrow$
  $\langle S \sqcup_S S''; \text{ freeze } l \text{ after } Q \text{ with } \lambda x. e_0, \{e_0[x := d_2], e, \dots\}, \{d_2\} \cup H \rangle$,

  as we were required to show.

- Case E-FREEZE-FINAL:

  Given: $\langle S; \text{ freeze } l \text{ after } Q \text{ with } v, \{v \dots\}, H \rangle \longrightarrow \langle S[l \mapsto (d_1, \text{true})]; d_1 \rangle$.

  To show: $\langle S \sqcup_S S''; \text{ freeze } l \text{ after } Q \text{ with } v, \{v \dots\}, H \rangle \longrightarrow \langle S[l \mapsto (d_1, \text{true})] \sqcup_S S''; d_1 \rangle$.

  We will first show that

  $\langle S \sqcup_S S''; \text{ freeze } l \text{ after } Q \text{ with } v, \{v \dots\}, H \rangle \longrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \text{true})]; d_1 \rangle$

  and then show why this is sufficient.

  We proceed by cases on l:

  - $l \notin dom(S'')$:
    By assumption, $S[l \mapsto (d_1, \text{true})] \sqcup_S S'' \neq \top_S$.
    By Lemma 7, $S \sqsubseteq_S S[l \mapsto (d_1, \text{true})]$.
    Therefore $S \sqcup_S S'' \neq \top_S$.
    Hence, by Definition 7, $(S \sqcup_S S'')(l) = S(l)$.
    From the premises of E-FREEZE-FINAL, we have that $S(l) = (d_1, frz_1)$.

Hence $(S \sqcup_S S'')(l) = (d_1, frz_1)$.

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

$\langle S \sqcup_S S''; \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ v, \{v \ldots\}, H\rangle \longrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \mathsf{true})]; d_1\rangle.$

- $l \in dom(S'')$:

  By assumption, $S[l \mapsto (d_1, \mathsf{true})] \sqcup_S S'' \neq \top_S$.

  By Lemma 7, $S \sqsubseteq_S S[l \mapsto (d_1, \mathsf{true})]$.

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

  Hence, by Definition 7, $(S \sqcup_S S'')(l) = S(l) \sqcup_p S''(l)$.

  From the premises of E-FREEZE-FINAL, we have that $S(l) = (d_1, frz_1)$.

  By assumption, $S[l \mapsto (d_1, \mathsf{true})] \sqcup_S S'' =_{frz} S$.

  Therefore $frz_1 = \mathsf{true}$.

  Therefore $S(l) = (d_1, \mathsf{true})$.

  Therefore $(S \sqcup_S S'')(l) = (d_1, \mathsf{true}) \sqcup_p S''(l)$.

  We proceed by cases on $S''(l)$:

  * $S''(l) = (d_3, \mathsf{false})$, where $d_3 \sqsubseteq d_1$:

    By Definition 6, $(d_1, \mathsf{true}) \sqcup_p (d_3, \mathsf{false}) = (d_1, \mathsf{true})$.

    Therefore $(S \sqcup_S S'')(l) = (d_1, \mathsf{true})$.

    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

    $\langle S \sqcup_S S''; \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ v, \{v \ldots\}, H\rangle \longrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \mathsf{true})]; d_1\rangle.$

  * $S''(l) = (d_3, \mathsf{false})$, where $d_3 \not\sqsubseteq d_1$:

    By Definition 6, $(d_1, \mathsf{true}) \sqcup_p (d_3, \mathsf{false}) = (\top, \mathsf{false})$.

    Therefore $S(l) \sqcup_p S''(l) = (\top, \mathsf{false})$.

    By Definition 1, $(\top, \mathsf{false}) = \top_p$.

    Therefore $S(l) \sqcup_p S''(l) = \top_p$.

    Therefore, by Definition 7, $S \sqcup_S S'' = \top_S$.

    This is a contradiction.

    Therefore,

    $\langle S \sqcup_S S''; \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ v, \{v \ldots\}, H\rangle \longrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \mathsf{true})]; d_1\rangle.$

  * $S''(l) = (d_3, \mathsf{true})$, where $d_3 = d_1$:

    By Definition 6, $(d_1, \mathsf{true}) \sqcup_p (d_3, \mathsf{true}) = (d_1, \mathsf{true})$.

    Therefore $(S \sqcup_S S'')(l) = (d_1, \mathsf{true})$.

    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

    $\langle S \sqcup_S S''; \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ v, \{v \ldots\}, H\rangle \longrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \mathsf{true})]; d_1\rangle.$

  * $S''(l) = (d_3, \mathsf{true})$, where $d_3 \neq d_1$:

    By Definition 6, $(d_1, \mathsf{true}) \sqcup_p (d_3, \mathsf{true}) = (\top, \mathsf{false})$.

    Therefore $S(l) \sqcup_p S''(l) = (\top, \mathsf{false})$.

    By Definition 1, $(\top, \mathsf{false}) = \top_p$.

    Therefore $S(l) \sqcup_p S''(l) = \top_p$.

    Therefore, by Definition 7, $S \sqcup_S S'' = \top_S$.

    This is a contradiction.

    Therefore,

    $\langle S \sqcup_S S''; \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ v, \{v \ldots\}, H\rangle \longrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \mathsf{true})]; d_1\rangle.$

In each case we have shown that

$\langle S \sqcup_S S''; \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ v, \{v \ldots\}, H\rangle \longrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \mathsf{true})]; d_1\rangle.$

Note that:

$$
\begin{aligned}
(S \sqcup_S S'')[l \mapsto (d_1, \mathsf{true})] &= S[l \mapsto (d_1, \mathsf{true})] \sqcup_S S''[l \mapsto (d_1, \mathsf{true})] \\
&= S \sqcup_S [l \mapsto (d_1, \mathsf{true})] \sqcup_S S'' \sqcup_S [l \mapsto (d_1, \mathsf{true})] \\
&= S \sqcup_S [l \mapsto (d_1, \mathsf{true})] \sqcup_S S'' \\
&= S[l \mapsto (d_1, \mathsf{true})] \sqcup_S S''.
\end{aligned}
$$

Therefore

$\langle S \sqcup_S S''; \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ v, \{v \ldots\}, H \rangle \longrightarrow \langle S[l \mapsto (d_1, \mathsf{true})] \sqcup_S S''; d_1 \rangle$,

as we were required to show.

- Case E-FREEZE-SIMPLE:

  Given: $\langle S; \texttt{freeze}\ l \rangle \longrightarrow \langle S[l \mapsto (d_1, \mathsf{true})]; d_1 \rangle$.

  To show: $\langle S \sqcup_S S''; \texttt{freeze}\ l \rangle \longrightarrow \langle S[l \mapsto (d_1, \mathsf{true})] \sqcup_S S''; d_1 \rangle$.

  We will first show that

  $\langle S \sqcup_S S''; \texttt{freeze}\ l \rangle \longrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \mathsf{true})]; d_1 \rangle$

  and then show why this is sufficient.

  We proceed by cases on l:

  - $l \notin dom(S'')$:

    By assumption, $S[l \mapsto (d_1, \mathsf{true})] \sqcup_S S'' \neq \top_S$.

    By Lemma 7, $S \sqsubseteq_S S[l \mapsto (d_1, \mathsf{true})]$.

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

    Hence, by Definition 7, $(S \sqcup_S S'')(l) = S(l)$.

    From the premise of E-FREEZE-SIMPLE, we have that $S(l) = (d_1, frz_1)$.

    Therefore, by E-FREEZE-SIMPLE, we have that

    $\langle S \sqcup_S S''; \texttt{freeze}\ l \rangle \longrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \mathsf{true})]; d_1 \rangle$.

  - $l \in dom(S'')$:

    By assumption, $S[l \mapsto (d_1, \mathsf{true})] \sqcup_S S'' \neq \top_S$.

    By Lemma 7, $S \sqsubseteq_S S[l \mapsto (d_1, \mathsf{true})]$.

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

    Hence, by Definition 7, $(S \sqcup_S S'')(l) = S(l) \sqcup_p S''(l)$.

    From the premise of E-FREEZE-SIMPLE, we have that $S(l) = (d_1, frz_1)$.

    By assumption, $S[l \mapsto (d_1, \mathsf{true})] \sqcup_S S'' =_{frz} S$.

    Therefore $frz_1 = \mathsf{true}$.

    Therefore $(S \sqcup_S S'')(l) = (d_1, \mathsf{true}) \sqcup_p S''(l)$.

    We proceed by cases on $S''(l)$:

    * $S''(l) = (d_2, \mathsf{false})$, where $d_2 \sqsubseteq d_1$:

      By Definition 6, $(d_1, \mathsf{true}) \sqcup_p (d_2, \mathsf{false}) = (d_1, \mathsf{true})$.

      Therefore $(S \sqcup_S S'')(l) = (d_1, \mathsf{true})$.

      Therefore, by E-FREEZE-SIMPLE, we have that

      $\langle S \sqcup_S S''; \texttt{freeze}\ l \rangle \longrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \mathsf{true})]; d_1 \rangle$.

    * $S''(l) = (d_2, \mathsf{false})$, where $d_2 \not\sqsubseteq d_1$:

      By Definition 6, $(d_1, \mathsf{true}) \sqcup_p (d_2, \mathsf{false}) = (\top, \mathsf{false})$.

      By Definition 1, $(\top, \mathsf{false}) = \top_p$.

      Therefore $S(l) \sqcup_p S''(l) = \top_p$.

Therefore, by Definition 7, $S \sqcup_S S'' = \top_S$.
This is a contradiction.
Therefore,
$\langle S \sqcup_S S''; \; \texttt{freeze } l \rangle \longrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \textsf{true})]; \; d_1 \rangle$.

* $S''(l) = (d_2, \textsf{true})$, where $d_2 = d_1$:
  Therefore $(S \sqcup_S S'')(l) = (d_1, \textsf{true}) \sqcup_p (d_2, \textsf{true})$.
  By Definition 6, $(d_1, \textsf{true}) \sqcup_p (d_2, \textsf{true}) = (d_1, \textsf{true})$.
  Therefore $(S \sqcup_S S'')(l) = (d_1, \textsf{true})$.
  Therefore, by E-FREEZE-SIMPLE, we have that
  $\langle S \sqcup_S S''; \; \texttt{freeze } l \rangle \longrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \textsf{true})]; \; d_1 \rangle$.

* $S''(l) = (d_2, \textsf{true})$, where $d_2 \neq d_1$:
  By Definition 6, $(d_1, \textsf{true}) \sqcup_p (d_2, \textsf{true}) = (\top, \textsf{false})$.
  By Definition 1, $(\top, \textsf{false}) = \top_p$.
  Therefore $S(l) \sqcup_p S''(l) = \top_p$.
  Therefore, by Definition 7, $S \sqcup_S S'' = \top_S$.
  This is a contradiction.
  Therefore,
  $\langle S \sqcup_S S''; \; \texttt{freeze } l \rangle \longrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \textsf{true})]; \; d_1 \rangle$.

In each case we have shown that

$\langle S \sqcup_S S''; \; \texttt{freeze } l \rangle \longrightarrow \langle (S \sqcup_S S'')[l \mapsto (d_1, \textsf{true})]; \; d_1 \rangle$.

Note that:

$$
\begin{aligned}
(S \sqcup_S S'')[l \mapsto (d_1, \textsf{true})] &= S[l \mapsto (d_1, \textsf{true})] \sqcup_S S''[l \mapsto (d_1, \textsf{true})] \\
&= S \sqcup_S [l \mapsto (d_1, \textsf{true})] \sqcup_S S'' \sqcup_S [l \mapsto (d_1, \textsf{true})] \\
&= S \sqcup_S [l \mapsto (d_1, \textsf{true})] \sqcup_S S'' \\
&= S[l \mapsto (d_1, \textsf{true})] \sqcup_S S''.
\end{aligned}
$$

Therefore $\langle S \sqcup_S S''; \; \texttt{freeze } l \rangle \longrightarrow \langle S[l \mapsto (d_1, \textsf{true})] \sqcup_S S''; \; d_1 \rangle$, as we were required to show.

$\square$

B.4 Stability Preservation

Definition 8 (Stable Configurations). A configuration $\langle S; \; e \rangle$ is *stable* if the free locations of e are a subset of $dom(S)$.

Lemma 8 (Stability Preservation). *If σ is stable and $\sigma \longrightarrow \sigma'$, then σ' is stable.*

Proof. Routine induction on the derivation of the reduction relation. $\square$

B.5 Renaming

Lemma 9 (Renaming). *If π is a permutation and $\sigma \longrightarrow \sigma'$, then $\pi(\sigma) \longrightarrow \pi(\sigma')$.*

Proof. Routine induction on the derivation of the reduction relation. $\square$

In the proof of confluence (*i.e.*, all following theorems), we implicitly assume that all configurations mentioned are stable.

B.6 Reordering

Lemma 10 (Reordering). *If $\langle S;\, e_a \rangle \longrightarrow \langle S_a;\, e_a' \rangle$ and $\langle S;\, e_b \rangle \longrightarrow \langle S_b;\, e_b' \rangle$, then either*

- *There exists S' and permutations π_a and π_b such that $\pi_a(S) = \pi_b(S) = S$ and*

  1. *$\langle \pi_b(S_b);\, e_a \rangle \longrightarrow \langle S';\, \pi_a(e_a') \rangle$ and*
  2. *$\langle \pi_a(S_a);\, e_b \rangle \longrightarrow \langle S';\, \pi_b(e_b') \rangle$ and*
  3. *$\pi_b(\pi_a(e_a')) = \pi_a(e_a')$ and $\pi_a(\pi_b(e_b')) = \pi_b(e_b')$,*

  or

- *$\langle S_b;\, e_a \rangle \longrightarrow$ **error** or $\langle S_a;\, e_b \rangle \longrightarrow$ **error**.*

Proof. Assume $D_a :: \langle S;\, e_a \rangle \longrightarrow \langle S_a;\, e_a' \rangle$ and $D_b :: \langle S;\, e_b \rangle \longrightarrow \langle S_b;\, e_b' \rangle$.
Now, consider whether $S_a =_{frz} S$ and $S_b =_{frz} S$.

- If $S_a =_{frz} S$ and $S_b =_{frz} S$:

  Let $\Delta_a = dom(S_a) - dom(S)$ and let $\Delta_b = dom(S_b)$.
  Suppose $\Delta_a = \{l_1, \ldots, l_n\}$.
  Now choose $L = \{l_1', \ldots, l_n'\}$ such that $l_i' \notin dom(S_a) \cup dom(S_b)$.
  Suppose $\Delta_b = \{m_1, \ldots, m_k\}$.
  Now choose $M = \{m_1', \ldots, m_k'\}$ such that $m_i' \notin dom(S_a) \cup dom(S_b) \cup L$.
  Let $\pi_a = (l_1\ l_1') \cdots (l_n\ l_n')$.
  Let $\pi_b = (m_1\ m_1') \cdots (m_k\ m_k')$.
  Since $\Delta_a \cap dom(S) = \emptyset$, we know that $\pi_a(S) = S$.
  Since $\Delta_b \cap dom(S) = \emptyset$, we know that $\pi_b(S) = S$.

  By renaming (Lemma 9), $\langle S;\, e_a \rangle \longrightarrow \langle \pi_a(S_a);\, \pi_a(e_a') \rangle$.
  By renaming (Lemma 9), $\langle S;\, e_b \rangle \longrightarrow \langle \pi_b(S_b);\, \pi_b(e_b') \rangle$.
  So we know that $\pi_a(e_a')$ is supported by $dom(\pi_a(S_a))$.
  So we know that $\pi_b(e_b')$ is supported by $dom(\pi_b(S_b))$.
  Hence $\pi_b(\pi_a(e_a')) = \pi_a(e_a')$, since π_b is the identity on S, and does not act on L.
  Hence $\pi_a(\pi_b(e_b')) = \pi_a(e_a')$, since π_a is the identity on S, and does not act on M.

  Furthermore, we know that $\pi_b(S_b)$ does not conflict with $\langle S;\, e_a \rangle \longrightarrow \langle \pi_a(S_a);\, \pi_a(e_a') \rangle$.
  This contradicts the construction of π:
  Assume an $l \in (dom(\pi_a(S_a)) - dom(S)) \cap (dom(\pi(S_b)) - dom(S))$.
  Then $l \in (dom(\pi_a(S_a)) - dom(S))$ and $l \in (dom(\pi(S_b)) - dom(S))$.
  Hence $l = l_i'$ for some $l_i' \in L$, since $l \in (dom(\pi_a(S_a)) - dom(S))$.
  But since $l \in (dom(\pi(S_b)) - dom(S))$, we know $l \in M$, a contradiction, since that implies $l \notin L$.

  Symmetrically, we know that $\pi_a(S_a)$ does not conflict with $\langle S;\, e_b \rangle \longrightarrow \langle \pi_b(S_b);\, \pi_b(e_b') \rangle$.
  If it did, then there is an $l \in (dom(\pi_a(S_a)) - dom(S)) \cap (dom(\pi_b(S_b)) - dom(S))$.
  Again, this contradicts the construction of π_a and π_b.

  Next, we know by monotonicity (Lemma 7) that $S \sqsubseteq_S \pi_a(S_a)$ and $S \sqsubseteq_S \pi_b(S_b)$.
  Hence $S \sqcup_S \pi_a(S_a) = \pi_a(S_a)$ and $S \sqcup_S \pi_b(S_b) = \pi_b(S_b)$.

  Now consider whether $\pi_a(S_a) \sqcup_S \pi_b(S_b) = \top_S$.

- Case $\pi_a(S_a) \sqcup_S \pi_b(S_b) \neq \top_S$:

  By independence (Lemma 3), $\langle S \sqcup_S \pi_a(S_a); e_b \rangle \longrightarrow \langle \pi_b(S_b) \sqcup_S \pi_a(S_a); \pi_b(e_b') \rangle$.
  By independence (Lemma 3), $\langle S \sqcup_S \pi_b(S_b)); e_a \rangle \longrightarrow \langle \pi_a(S_a) \sqcup_S \pi_b(S_b); \pi_a(e_a') \rangle$.
  So $\langle \pi_a(S_a); e_b \rangle \longrightarrow \langle \pi_b(S_b) \sqcup_S \pi_a(S_a); \pi_b(e_b') \rangle$.
  So $\langle \pi_b(S_b); e_a \rangle \longrightarrow \langle \pi_a(S_a) \sqcup_S \pi_b(S_b); \pi_a(e_a') \rangle$.
  We take $S' = \pi_a(S_a) \sqcup_S \pi_b(S_b)$, $\pi_a = \pi$ and $\pi_b = id$ as witnesses.

- Case $\pi_a(S_a) \sqcup_S \pi_b(S_b) = \top_S$:

  By definition, there is an l such that $\pi_a(S_a)(l) \sqcup_p \pi_b(S_b)(l) = \top_p$.
  From the construction of π, it follows that $l \in dom(S)$.
  Since $\pi_a(S) = S$, it follows that $\pi_a(S_a)(l) = S_a(l)$.

  We know $S \sqcup_S \pi_a(S_a) = \pi_a(S_a)$ and $S \sqcup_S \pi_b(S_b) = \pi_b(S_b)$.

  We now show that $\pi_a(S_a)(l) \neq S(l)$, and $\pi_b(S_b)(l) \neq S(l)$.
  Suppose $\pi_a(S_a)(l) = S(l)$.
  Then $S(l) \sqcup_p \pi_b(S_b)(l) = \top_p$, since $\pi_a(S_a)(l) \sqcup_p \pi_b(S_b)(l) = \top_p$.
  But we know that $S \sqcup_S \pi_b(S_b) = \pi_b(S_b)$, and so $S(l) \sqcup_p \pi_b(S_b)(l) = \pi_b(S_b)(l)$.
  This is a contradiction, and so $\pi_a(S_a)(l) \neq S(l)$.
  Similarly, $\pi_b(S_b)(l) \neq S(l)$.

  The only rule which changes the store, without changing status, is E-PUT.
  Hence D_a and D_b end in E-PUT.
  So $e_a = \text{put } l\ \pi_a(S_a)(l)$ and $e_b = \text{put } l\ \pi_b(S_b)(l)$.
  Since $\pi_a(S_a)(l) = l$, we also know that $e_a = \text{put } l\ S_a(l)$.
  By E-PUT-ERR, $\langle S_a; \text{put } l\ \pi_b(S_b)(l) \rangle \longrightarrow$ **error**.

- Case $S_a \neq_{frz} S$ or $S_b \neq_{frz} S$:

  Without loss of generality, suppose that $S_a \neq_{frz} S$.
  The only rule which changes the status of the store is E-FREEZE-FINAL.
  Hence D_a uses the E-FREEZE-FINAL.
  Hence $e_a = \text{freeze } l \text{ after } Q \text{ with } v, \{v \ldots\}, H$.
  Hence $S(l) = (d, \text{false})$.
  Hence $e_a' = d$.
  Hence $S_a = S[l \mapsto (d, \text{true})]$.
  Now we proceed by cases on D_b.

  - Case E-BETA:

    In this case, $e_b = \lambda x.\, e\ v$ and $e_b' = [v/x]e$ and $S_b = S$.
    We take the witness $S' = S_a$ and $\pi = id$.
    By rule E-APP, $\langle S_a; \lambda x.\, e\ v \rangle \longrightarrow \langle S_a; [v/x]e \rangle$.
    Hence $\langle S_a; e_b \rangle \longrightarrow \langle S'; e_b' \rangle$.
    By assumption $\langle S; e_a \rangle \longrightarrow \langle S_a; e_a' \rangle$.
    Hence $\langle S_b; e_a \rangle \longrightarrow \langle S'; e_a' \rangle$.

  - Case E-NEW:

    In this case, $e_b = \text{new}$ and $e_b' = l$ and $S_b = S[l' \mapsto (\bot, \text{false})]$, where $l \notin dom(S)$.
    Since $dom(S) = dom(S_a)$, we know $l \notin dom(S_a)$.
    By rule E-NEW, $\langle S_a; \text{new} \rangle \longrightarrow S_a[l' \mapsto (\bot, \text{false})]l'$. By rule E-FREEZE-FINAL, $\langle S_b; e_a \rangle \longrightarrow \langle S_a[l' \mapsto (\bot, \text{false})]; d \rangle$.
    We can take $S' = S_a[l' \mapsto (\bot, \text{false})]$ and $\pi_a = \pi_b = id$.

– Case E-PUT:

In this case, $e_b = \texttt{put } l' \, d'$. In this case, $e'_b = \texttt{()}$.
In this case, $p_1 = S(l')$.
In this case, $p_2 = p_1 \sqcup_p (d, \mathsf{false}) \neq \top$.
In this case, $S_b = S[l' \mapsto p_2]$. Now consider whether $l = l'$:

* Case $l \neq l'$:
  Take $\pi_a = \pi_b = id$, and $S' = S_a[l' \mapsto p_2]$.
  Since $l \neq l'$, $p_1 = S_a(l')$.
  By rule E-PUT, $\langle S_a; \, e_b \rangle \longrightarrow \langle S'; \, e'_b \rangle$.
  By rule E-FREEZE-FINAL, $\langle S_b; \, e_a \rangle \longrightarrow \langle S'; \, e'_a \rangle$.

* Case $l = l'$:
  Consider whether $d' \leq d$:

  · Case $d' \leq d$:
    First, note that $S_b = S$, since $(d, \mathsf{false}) \sqcup_p (d', \mathsf{false}) = (d, \mathsf{false})$.
    Next, note that $S_a(l) = (d, \mathsf{true})$.
    By definition, $(d, \mathsf{true}) \sqcup_p (d', \mathsf{false}) = (d, \mathsf{true})$.
    So take $S' = S_a$ and $\pi_a = \pi_b = id$.
    By rule E-PUT, $\langle S_a; \, e_b \rangle \longrightarrow \langle S'; \, e'_b \rangle$.
    By rule E-FREEZE-FINAL, $\langle S_b; \, e_a \rangle \longrightarrow \langle S'; \, e'_a \rangle$.

  · Case $d' > d$:
    Note that $S_a(l) = (d, \mathsf{true})$.
    By definition, $(d, \mathsf{true}) \sqcup_p (d', \mathsf{false}) = \top_p$.
    By rule E-PUT-ERR, $\langle S_a; \, e_b \rangle \longrightarrow$ **error**.

* Case E-PUT-ERR:
  Can't happen.

* Case E-GET:
  We take $S' = S_a$ and $\pi_a = \pi_b = id$.

  By inversion, we get $e_b = \texttt{get } l' \, P$, and $S(l') = p_1$, and $incomp(P)$
  and $p_2 \in P$ and $p_2 \sqsubseteq_p p_1$ and $e'_b = p_2$ and $S_b = S$.
  Since $S_b = S$, by equality $\langle S_b; \, e_a \rangle \longrightarrow \langle S'; \, e'_a \rangle$.

  By monotonicity, $S \sqsubseteq_S S_a$.
  Hence $S(l') \sqsubseteq_p S_a(l')$.
  Hence we can take $p'_1 = S_a(l')$ and then $p_2 \sqsubseteq_p p'_1$ by transitivity. By rule E-GET, $\langle S_a; \, e_b \rangle \longrightarrow S_a p_2$.
  So $\langle S_a; \, e_b \rangle \longrightarrow \langle S'; \, e'_b \rangle$.

* Case E-FREEZE-INIT:
  By inversion, $e_b = \texttt{freeze } l \texttt{ after } Q' \texttt{ with } \lambda x.\, e$.
  By inversion, $e'_b = \texttt{freeze } l \texttt{ after } Q' \texttt{ with } \lambda x.\, e, \emptyset, \emptyset$.
  By inversion, $S_b = S$.

  Take $\pi_a = \pi_b = id$ and $S' = S_a$.
  By rule E-FREEZE-INIT, $\langle S_a; \, e_b \rangle \longrightarrow \langle S'; \, e'_b \rangle$.
  Since $S_b = S$, $D_a :: \langle S_b; \, e_a \rangle \longrightarrow \langle S'; \, e'_a \rangle$.

* Case E-SPAWN-HANDLER:
  Take $\pi_a = \pi_b = id$ and $S' = S_a$.

  By inversion, $e_b = \texttt{freeze } l' \texttt{ after } Q' \texttt{ with } \lambda x.\, e_0, \{e, \ldots\}, H'$.
  By inversion, $e'_b = \texttt{freeze } l' \texttt{ after } Q' \texttt{ with } \lambda x.\, e_0, \{[d_2/x]e_0, e, \ldots\}, H'$.
  By inversion, $S_b = S$.

By inversion, $S(l) = (d_1, frz_1)$ and $d_2 \sqsubseteq d_1$ and $d_2 \notin H'$ and $d_2 \in Q'$.

By monotonicity (Lemma 7), $S \sqcup_S S_a$.
Hence $S_a(l) = (d_1', frz_1')$ such that $(d_1, frz_1) \sqsubseteq_p (d', frz')$.
Hence $d_2 \sqsubseteq d_1'$.
Hence by rule E-SPAWN-HANDLER, $\langle S_a; e_b \rangle \longrightarrow \langle S'; e_b' \rangle$.
Since $S_b = S$, we know $\langle S_b; e_a \rangle \longrightarrow \langle S'; e_a' \rangle$.

* Case E-FREEZE-FINAL:
  By inversion, $e_b = $ freeze l' after Q' with $v', \{v', \ldots\}, H'$.
  By inversion, $S(l') = (d_1', frz_1')$.
  By inversion, $\forall d_2' \sqsubseteq d_1'. d_2' \in Q' \implies d_2' \in H'$.
  By inversion, $S_b = S[l' \mapsto (d_1', \mathsf{true})]$.
  By inversion, $e_b' = d_1'$.
  Consider whether $l = l'$:

  · Case $l \neq l'$: In this case, define $S' = S_a[l' \mapsto (d_1', \mathsf{true})]$, and $\pi_a = \pi_b = id$.
    Note that $S_a(l') = S(l')$ and $S_b(l) = S(l)$.
    Then by rule E-FREEZE-FINAL, $\langle S_a; e_b \rangle \longrightarrow \langle S'; e_b' \rangle$.
    Then by rule E-FREEZE-FINAL, $\langle S_b; e_a \rangle \longrightarrow \langle S'; e_a' \rangle$.

  · Case $l = l'$: In this case, $d_1 = d_1'$.
    Hence $S_b = S_a$.
    Take $S' = S_a$ and $\pi_a = \pi_b = id$.

    We know $S_a(l) = (d_1', \mathsf{true})$.
    So we know $\forall d_2' \sqsubseteq d_1'. d_2' \in Q' \implies d_2' \in H'$.
    By rule E-FREEZE-FINAL, $\langle S_a; e_b \rangle \longrightarrow \langle S'; e_b' \rangle$.

    We know $S_b(l) = (d_1, \mathsf{true})$.
    So we know $\forall d_2 \sqsubseteq d_1. d_2 \in Q \implies d_2 \in H$.
    By rule E-FREEZE-FINAL, $\langle S_b; e_a \rangle \longrightarrow \langle S'; e_a' \rangle$.

* Case E-FREEZE-SIMPLE:
  By inversion, $e_b = $ freeze l'.
  By inversion, $S(l') = (d_1', frz_1')$.
  By inversion, $S_b = S[l' \mapsto (d_1', \mathsf{true})]$.
  By inversion, $e_b' = d_1'$.
  Consider whether $l = l'$:

  · Case $l \neq l'$: In this case, define $S' = S_a[l' \mapsto (d_1', \mathsf{true})]$, and $\pi_a = \pi_b = id$.
    Note that $S_a(l') = S(l')$ and $S_b(l) = S(l)$.
    Then by rule E-FREEZE-FINAL, $\langle S_a; e_b \rangle \longrightarrow \langle S'; e_b' \rangle$.
    Then by rule E-FREEZE-FINAL, $\langle S_b; e_a \rangle \longrightarrow \langle S'; e_a' \rangle$.

  · Case $l = l'$: In this case, $d_1 = d_1'$.
    Hence $S_b = S_a$.
    Take $S' = S_a$ and $\pi_a = \pi_b = id$.

    We know $S_a(l) = (d_1', \mathsf{true})$.
    By rule E-FREEZE-SIMPLE, $\langle S_a; e_b \rangle \longrightarrow \langle S'; e_b' \rangle$.

    We know $S_b(l) = (d_1, \mathsf{true})$.
    So we know $\forall d_2 \sqsubseteq d_1. d_2 \in Q \implies d_2 \in H$.
    By rule E-FREEZE-FINAL, $\langle S_b; e_a \rangle \longrightarrow \langle S'; e_a' \rangle$.

$\square$

B.7 Context Extension

Lemma 11 (Context Extension). *If $\langle S; e \rangle \longrightarrow \langle S'; e' \rangle$, then $\langle S; E[e] \rangle \longrightarrow \langle S'; E[e'] \rangle$.*

Proof. Consider whether $\langle S; e \rangle \longrightarrow \langle S'; e' \rangle$ steps by the E-EVAL-CTXT rule or not.

- Case $\langle S; E_0[e] \rangle \longrightarrow \langle S'; E_0[e'_0] \rangle$.
  By inversion, $\langle S; e \rangle \longrightarrow \langle S'; e'_0 \rangle$.
  By rule E-EVAL-CTXT with the context $E[E_0[\,]\,]$, $\langle S; E[E_0[e]] \rangle \longrightarrow \langle S'; E[E_0[e'_0]] \rangle$.

- Otherwise:

  In this case e is a reducible expression.
  By rule E-EVAL-CTXT with the context E, $\langle S; E[e] \rangle \longrightarrow \langle S'; E[e'] \rangle$.

$\square$

B.8 Contextual Reordering

Lemma 12 (Contextual Reordering). *If $\sigma \equiv \langle S; e \rangle \longrightarrow \sigma_a$ and $\sigma \longrightarrow \sigma_b$ using the E-EVAL-CTXT rules, then either*

- *there exists π_a and π_b such that $\pi_a(S) = \pi_b(S) = S$ and σ' such that $\pi_a(\sigma_a) \longrightarrow \sigma'$ and $\pi_b(\sigma_b) \longrightarrow \sigma'$, or*

- $\sigma_a \longrightarrow$ **error** *or* $\sigma_b \longrightarrow$ **error**.

Proof. By inversion, we get $\sigma = \langle S; e \rangle$, with $e = E_a[e_a] = E_b[e_b]$,
and $\sigma_a = \langle S_a; E_a[e'_a] \rangle$ and $\sigma_b = \langle S_b; E_b[e'_b] \rangle$,
and $\langle S; e_a \rangle \longrightarrow \langle S_a; e'_a \rangle$ and $\langle S; e_b \rangle \longrightarrow \langle S_b; e'_b \rangle$.

We proceed by induction on the sum of the heights of E_a and E_b, by cases on e:

- Case $e = x$:

  Impossible.

- Case $e = v$:

  Values can't step, so this case is impossible.

- Case e is reducible:

  Since e is reducible, so both contexts are $[\,]$.
  Hence the result follows from reordering (Lemma 10).

- Case $e = e_1 \; e_2$:

  Now, we proceed by cases on the shape of E_a and E_b:

  - $E_a = F_a \; e_2$ and $E_b = F_b \; e_2$.

    In this case $e_1 = F_a[e_a] = F_b[e_b]$.
    By rule E-EVAL-CTXT, $\langle S; F_a[e_a] \rangle \longrightarrow \langle S_a; F_a[e'_a] \rangle$.
    By rule E-EVAL-CTXT, $\langle S; F_b[e_b] \rangle \longrightarrow \langle S_b; F_b[e'_b] \rangle$.
    By induction, there exists an S', e'_1, π_a and π_b such that $\pi_a(S) = S$ and $\pi_b(S) = S$,
    and $\langle \pi_b(S_b); F_a[e_a] \rangle \longrightarrow \langle S'; e'_1 \rangle$ and $\langle \pi_a(S_a); F_a[e_a] \rangle \longrightarrow \langle S'; e'_1 \rangle$.
    By context extension (Lemma 11), $\langle \pi_b(S_b); F_a[e_a] \; e_2 \rangle \longrightarrow \langle S'; e'_1 \; e_2 \rangle$.
    By context extension (Lemma 11), $\langle \pi_a(S_a); F_b[e_b] \; e_2 \rangle \longrightarrow \langle S'; e'_1 \; e_2 \rangle$.
    Hence $\langle \pi_b(S_b); E_a[e_a] \rangle \longrightarrow \langle S'; e'_1 \; e_2 \rangle$ and $\langle \pi_a(S_a); E_b[e_b] \rangle \longrightarrow \langle S'; e'_1 \; e_2 \rangle$.

– $E_a = e_1\ F_a$ and $E_b = e_1\ F_b$.

  Similar to the previous case.

– $E_a = F_a\ e_2$ and $E_b = e_1; F_b$.
  Then $e_1\ e_2 = F_a[e_a]\ F_b[e_b]$.
  By reordering, we have π_a and π_b such that $\pi_a(S) = \pi_b(S)$ and
  $\langle \pi_a(S_a); e_b \rangle \longrightarrow \langle S'; \pi_b(e_b') \rangle$ and
  $\langle \pi_b(S_b); e_a \rangle \longrightarrow \langle S'; \pi_a(e_a') \rangle$ and
  $\pi_a(\pi_b(e_b')) = \pi_b(e_b')$ and $\pi_b(\pi_a(e_a')) = \pi_a(e_a')$.
  By E-EVAL-CTXT with $E = F_a[\pi_a(e_a')]\ F_b$, $\langle \pi_a(S_a); E[e_b] \rangle \longrightarrow \langle S'; E[\pi_b(e_b')] \rangle$.
  By E-EVAL-CTXT with $E' = F_a\ F_b[\pi_b(e_b')]$, $\langle \pi_b(S_b); E'[e_a] \rangle \longrightarrow \langle S'; E'[\pi_a(e_a')] \rangle$.
  Observe that $E[\pi_b(e_b')] = E'[\pi_a(e_a')]$.

– $E_a = e_1\ F_a$ and $E_b = F_b\ e_2$.

  Similar to the previous case.

- Case $e = \texttt{get}\ e_1\ e_2$:

  Similar to the previous case.

- Case $e = \texttt{put}\ e_1\ e_2$:

  Similar to the previous case.

- Case $e = \texttt{freeze}\ e_1$:

  In this case, we can see that $E_a = \texttt{freeze}\ F_a[e_a]$ and $E_b = \texttt{freeze}\ F_b[e_b]$.
  We may assume E_a and E_b are not $[\,]$ since we've already handled the case when e is reducible.
  In this case $e_1 = F_a[e_a] = F_b[e_b]$.
  By rule E-EVAL-CTXT, $\langle S; F_a[e_a] \rangle \longrightarrow \langle S_a; F_a[e_a'] \rangle$.
  By rule E-EVAL-CTXT, $\langle S; F_b[e_b] \rangle \longrightarrow \langle S_b; F_b[e_b'] \rangle$.
  By induction, there exists an S', e_1', π_a and π_b such that $\pi_a(S) = S$ and $\pi_b(S) = S$,
  and $\langle \pi_b(S_b); F_a[e_a] \rangle \longrightarrow \langle S'; e_1' \rangle$ and $\langle \pi_a(S_a); F_a[e_a] \rangle \longrightarrow \langle S'; e_1' \rangle$.
  By context extension (Lemma 11), $\langle \pi_b(S_b); \texttt{freeze}\ F_a[e_a] \rangle \longrightarrow \langle S'; \texttt{freeze}\ e_1' \rangle$.
  By context extension (Lemma 11), $\langle \pi_a(S_a); \texttt{freeze}\ F_b[e_b] \rangle \longrightarrow \langle S'; \texttt{freeze}\ e_1' \rangle$.

- Case $\texttt{freeze}\ e_1\ \texttt{after}\ e_2\ \texttt{with}\ e_3$:

  Similar to the application case.

- Case $\texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\,t, \{t_1, \ldots, t_n\}, H$:

  In this case, $E_a = \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\,t, \{t_1, \ldots, F_a, \ldots, t_n\}, H$.
  In this case, $E_b = \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\,t, \{t_1, \ldots, F_a, \ldots, t_n\}, H$.
  There are two possibilities, depending on whether or not F_a and F_b are at the same position i or not.

  – Same subterm:
    Then $e = \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\,t, \{t_1, \ldots, F_a[e_a], \ldots, t_n\}, H$.
    Then $e = \texttt{freeze}\ l\ \texttt{after}\ Q\ \texttt{with}\ \lambda x.\,t, \{t_1, \ldots, F_b[e_b], \ldots, t_n\}, H$.
    Then $t_i = F_a[e_a] = F_b[e_b]$.
    So by E-EVAL-CTXT, we have $\langle S; F_a[e_a] \rangle \longrightarrow \langle S_a; F_a[e_a'] \rangle$.
    So by E-EVAL-CTXT, we have $\langle S; F_b[e_b] \rangle \longrightarrow \langle S_b; F_b[e_b'] \rangle$.
    By induction, we have S', π_a, π_b and t_i' such that
    $\pi_a(S) = \pi_b(S) = S$ and
    $\langle \pi_b(S_b); F_a[e_a] \rangle \longrightarrow \langle S'; t_i' \rangle$ and

$\langle \pi_a(S_a); \, F_b[e_b] \rangle \longrightarrow \langle S'; \, t_i' \rangle.$

By context extension (Lemma 11), $\langle \pi_b(S_b); \, E_a[e_a] \rangle \longrightarrow \langle S'; \, \texttt{freeze} \, l \, \texttt{after} \, Q \, \texttt{with} \, \lambda x.\, t, \{t_1, \ldots, t_i', \ldots, t_n\}, H \rangle.$

By context extension (Lemma 11), $\langle \pi_a(S_a); \, E_b[e_b] \rangle \longrightarrow \langle S'; \, \texttt{freeze} \, l \, \texttt{after} \, Q \, \texttt{with} \, \lambda x.\, t, \{t_1, \ldots, t_i', \ldots, t_n\}, H \rangle.$

– $F_a[e_a]$ and $F_b[e_b]$ are different subterms:

Then $e = \texttt{freeze} \, l \, \texttt{after} \, Q \, \texttt{with} \, \lambda x.\, t, \{t_1, \ldots, F_a[e_a], \ldots, F_b[e_b], \ldots, t_n\}, H.$

By reordering, we have π_a and π_b such that $\pi_a(S) = \pi_b(S)$ and

$\langle \pi_a(S_a); \, e_b \rangle \longrightarrow \langle S'; \, \pi_b(e_b') \rangle$ and

$\langle \pi_b(S_b); \, e_a \rangle \longrightarrow \langle S'; \, \pi_a(e_a') \rangle$ and

$\pi_a(\pi_b(e_b')) = \pi_b(e_b')$ and $\pi_b(\pi_a(e_a')) = \pi_a(e_a').$

Let $E_a' = \texttt{freeze} \, l \, \texttt{after} \, Q \, \texttt{with} \, \lambda x.\, t, \{t_1, \ldots, F_a[\,], \ldots, F_b[\pi_b(e_b')], \ldots, t_n\}, H.$

Let $E_b' = \texttt{freeze} \, l \, \texttt{after} \, Q \, \texttt{with} \, \lambda x.\, t, \{t_1, \ldots, F_a[\pi_a(e_a')], \ldots, F_b[\,], \ldots, t_n\}, H.$

Let $e' = \texttt{freeze} \, l \, \texttt{after} \, Q \, \texttt{with} \, \lambda x.\, t, \{t_1, \ldots, F_a[\pi_a(e_a')], \ldots, F_b[\pi_b(e_b')], \ldots, t_n\}, H.$

Note that $e' = E_a'[\pi_a(e_a')] = E_b'[\pi_b(e_b')].$

By rule E-EVAL-CTXT, $\langle \pi_b(S_b); \, E_a'[e_a] \rangle \longrightarrow \langle S'; \, e' \rangle.$

By rule E-EVAL-CTXT, $\langle \pi_a(S_a); \, E_b'[e_b] \rangle \longrightarrow \langle S'; \, e' \rangle.$

$\square$

B.9 Strong Local Quasi-Diamond

Lemma 13 (Strong Local Quasi-Diamond). *If $\sigma \equiv \langle S; \, e \rangle \longrightarrow \sigma_a$ and $\sigma \longrightarrow \sigma_b$, then either:*

1. *there exist i, j, π_a, π_b and σ_c such that $\pi_a(S) = \pi_b(S) = S$ and $\pi_a(\sigma_a) \longrightarrow^i \sigma_c$ and $\pi_b(\sigma_b) \longrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$, or*

2. *$\sigma_a \longrightarrow \textbf{error}$ or $\sigma_b \longrightarrow \textbf{error}$.*

Proof. By induction on the size of the derivation of $\sigma \longrightarrow \sigma_a$, by cases on syntax of the term e in $\sigma = \langle S; \, e \rangle.$

- E-EVAL-CTXT: $\sigma = \langle S; \, E[e] \rangle$, and $\sigma_a = \langle S'; \, E[e'] \rangle.$

  Now, consider $\sigma \longrightarrow \sigma_b.$
  If it steps by the E-EVAL-CTXT rule, then we conclude with context reordering (Lemma 12), choosing $i = j = 1.$
  If it steps by another rule, then $E[e]$ is a reducible expression, and $E[-] = [\,].$
  Then the result follows by reordering (Lemma 10), choosing $i = j = 1.$

- E-BETA: $\sigma = \langle S; \, (\lambda x.\, e) \, v \rangle$, and $\sigma_a = \langle S; \, e[x := v] \rangle.$

  Given:

  – $\langle S; \, (\lambda x.\, e) \, v \rangle \longrightarrow \langle S; \, e[x := v] \rangle$, and
  – $\langle S; \, (\lambda x.\, e) \, v \rangle \longrightarrow \sigma_b.$

  To show: There exist σ_c, i, j such that

  $\langle S; \, e[x := v] \rangle \longrightarrow^i \sigma_c$ and $\sigma_b \longrightarrow^j \sigma_c$ 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 $\sigma_a = \langle S[l \mapsto (\bot, \textsf{false})]; \, l \rangle.$

  Given:

– $\langle S; \texttt{new} \rangle \longrightarrow \langle S[l \mapsto (\bot, \mathsf{false})]; \, l \rangle$, and

– $\langle S; \texttt{new} \rangle \longrightarrow \sigma_b$.

To show: There exist σ_c, i, j such that

$\langle S[l \mapsto (\bot, \mathsf{false})]; \, l \rangle \longrightarrow^i \sigma_c$ and $\sigma_b \longrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

By inspection of the operational semantics, $\sigma_b = \langle S[l' \mapsto (\bot, \mathsf{false})]; \, l' \rangle$.

From the side condition of E-NEW, $l \notin S$.

Therefore, in $\langle S[l' \mapsto (\bot, \mathsf{false})]; \, l' \rangle$, we can α-rename l' to l, resulting in $\langle S[l \mapsto (\bot, \mathsf{false})]; \, l \rangle$.

Choose $\sigma_c = \langle S[l \mapsto (\bot, \mathsf{false})]; \, l \rangle$, $i = 0$ 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 $\sigma_a = \langle S[l \mapsto p_2]; \ ( ) \rangle$.

  Given:

  – $\langle S; \texttt{put } l \ d_2 \rangle \longrightarrow \langle S[l \mapsto p_2]; \ ( ) \rangle$, and

  – $\langle S; \texttt{put } l \ d_2 \rangle \longrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that

  $\langle S[l \mapsto p_2]; \ ( ) \rangle \longrightarrow^i \sigma_c$ and $\sigma_b \longrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

  By inspection of the operational semantics, $\sigma_b = \langle S[l \mapsto p_2]; \ ( ) \rangle$.

  Choose $\sigma_c = \langle S[l \mapsto p_2]; \ ( ) \rangle$, $i = 0$ and $j = 0$.

  Then $\langle S[l \mapsto p_2]; \ ( ) \rangle = \sigma_c$ and $\sigma_b = \sigma_c$, as required.

- E-PUT-ERR: $\sigma = \langle S; \texttt{put } l \ d_2 \rangle$, and $\sigma_a = \mathbf{error}$.

  Given:

  – $\langle S; \texttt{put } l \ d_2 \rangle \longrightarrow \mathbf{error}$, and

  – $\langle S; \texttt{put } l \ d_2 \rangle \longrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that

  $\mathbf{error} \longrightarrow^i \sigma_c$ and $\sigma_b \longrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

  By inspection of the operational semantics, $\sigma_b = \mathbf{error}$.

  Choose $\sigma_c = \mathbf{error}$, $i = 0$ and $j = 0$.

  Then $\mathbf{error} = \sigma_c$ 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:

  – $\langle S; \texttt{get } l \ P \rangle \longrightarrow \langle S; \, p_2 \rangle$, and

  – $\langle S; \texttt{get } l \ P \rangle \longrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that

  $\langle S; \, p_2 \rangle \longrightarrow^i \sigma_c$ and $\sigma_b \longrightarrow^j \sigma_c$ 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: $\sigma = \langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e \rangle$, and $\sigma_a = \langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e, \{\}, \{\} \rangle$.
  Given:

  - $\langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e \rangle \longrightarrow \langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e, \{\}, \{\} \rangle$, and
  - $\langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e \rangle \longrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that

  $\langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e, \{\}, \{\} \rangle \longrightarrow^i \sigma_c$ and $\sigma_b \longrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

  By inspection of the operational semantics, $\sigma_b = \langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e, \{\}, \{\} \rangle$.

  Choose $\sigma_c = \langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e, \{\}, \{\} \rangle$, $i = 0$ and $j = 0$.

  Then $\langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e, \{\}, \{\} \rangle = \sigma_c$ and $\sigma_b = \sigma_c$, as required.

- E-SPAWN-HANDLER: $\sigma = \langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e_0, \{e, \ldots\}, H \rangle$, and
  $\sigma_a = \langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e, \ldots\}, \{d_2\} \cup H \rangle$.
  Given:

  - $\langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e_0, \{e, \ldots\}, H \rangle \longrightarrow$
    $\langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e, \ldots\}, \{d_2\} \cup H \rangle$, and
  - $\langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e_0, \{e, \ldots\}, H \rangle \longrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that

  $\langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e, \ldots\}, \{d_2\} \cup H \rangle \longrightarrow^i \sigma_c$ and $\sigma_b \longrightarrow^j \sigma_c$ and $i \leq 1$ and $j \leq 1$.

  By inspection of the operational semantics, one of the following possibilities must hold:

  - $\sigma \longrightarrow \sigma_b$ by E-SPAWN-HANDLER:
    Hence $\sigma_b = \langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e_0, \{e_0[x := d'_2], e, \ldots\}, \{d'_2\} \cup H \rangle$.
    Here, there are two subcases:

    * $d'_2 \neq d_2$:
      Choose:
      $\sigma_c = \langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e_0[x := d'_2], e, \ldots\}, \{d_2, d'_2\} \cup H \rangle$,
      $i = 1$ and $j = 1$.
      To show:

      1. $\sigma_a \longrightarrow \sigma_c$, where
         $\sigma_a = \langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e, \ldots\}, \{d_2\} \cup H \rangle$ and
         $\sigma_c = \langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e_0[x := d'_2], e, \ldots\}, \{d_2, d'_2\} \cup H \rangle$.
         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,
         $\langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e, \ldots\}, \{d_2\} \cup H \rangle \longrightarrow$
         $\langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e_0, \{e_0[x := d'_2], e_0[x := d_2], e, \ldots\}, \{d'_2\} \cup \{d_2\} \cup H \rangle$,
         which is equivalent to
         $\langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e_0[x := d'_2], e, \ldots\}, \{d_2, d'_2\} \cup H \rangle$.
         Hence $\sigma_a \longrightarrow \sigma_c$.
      2. $\sigma_b \longrightarrow \sigma_c$, where
         $\sigma_b = \langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e_0, \{e_0[x := d'_2], e, \ldots\}, \{d'_2\} \cup H \rangle$, and
         $\sigma_c = \langle S; \mathtt{freeze}\, l\, \mathtt{after}\, Q\, \mathtt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e_0[x := d'_2], e, \ldots\}, \{d_2, d'_2\} \cup H \rangle$.
         The proof is as follows:

From the premises of E-SPAWN-HANDLER,
$S(l) = (d_1, frz_1)$ and $d_2 \sqsubseteq d_1$ and $d_2 \notin H$ and $d_2 \in Q$.
Therefore, by E-SPAWN-HANDLER,
$\langle S; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2'], e, \dots\}, \{d_2'\} \cup H \rangle \longrightarrow$
$\langle S; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e_0[x := d_2'], e, \dots\}, \{d_2\} \cup \{d_2'\} \cup H \rangle$,
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 $\sigma_b \longrightarrow \sigma_c$.

* $d_2' = d_2$:
  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.

- $\sigma \longrightarrow \sigma_b$ by E-EVAL-CTXT:
  Hence $\sigma_b = \langle S'; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e', \dots\}, H \rangle$.
  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. $\sigma_a \longrightarrow \sigma_c$, where
     $\sigma_a = \langle S; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e, \dots\}, \{d_2\} \cup H \rangle$ and
     $\sigma_c = \langle S'; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e', \dots\}, \{d_2\} \cup H \rangle$.
     The proof is as follows:
     From the premise of E-EVAL-CTXT, $\langle S; e \rangle \longrightarrow \langle S'; e' \rangle$.
     From the definition of evaluation contexts,
     $\texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], [\,], \dots\}, \{d_2\} \cup H$
     is an evaluation context.
     Hence, by E-EVAL-CTXT,
     $\langle S; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e, \dots\}, \{d_2\} \cup H \rangle \longrightarrow$
     $\langle S'; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e', \dots\}, \{d_2\} \cup H \rangle$.
     Hence $\sigma_a \longrightarrow \sigma_c$.

  2. $\sigma_b \longrightarrow \sigma_c$, where
     $\sigma_b = \langle S'; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e', \dots\}, H \rangle$, and
     $\sigma_c = \langle S'; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e', \dots\}, \{d_2\} \cup H \rangle$.
     The proof is as follows:
     From the premises of E-SPAWN-HANDLER,
     $S(l) = (d_1, frz_1)$ and $d_2 \sqsubseteq d_1$ and $d_2 \notin H$ and $d_2 \in Q$.
     Hence, by E-SPAWN-HANDLER,
     $\langle S'; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e', \dots\}, H \rangle \longrightarrow$
     $\langle S'; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, \lambda x.\, e_0, \{e_0[x := d_2], e', \dots\}, \{d_2\} \cup H \rangle$.
     Hence $\sigma_b \longrightarrow \sigma_c$.

- E-FREEZE-FINAL: $\sigma = \langle S; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, v, \{v \dots\}, H \rangle$, and $\sigma_a = \langle S[l \mapsto (d_1, \mathsf{true})]; d_1 \rangle$.
  Given:

  - $\langle S; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, v, \{v \dots\}, H \rangle \longrightarrow \langle S[l \mapsto (d_1, \mathsf{true})]; d_1 \rangle$, and

  - $\langle S; \texttt{freeze}\, l\, \texttt{after}\, Q\, \texttt{with}\, v, \{v \dots\}, H \rangle \longrightarrow \sigma_b$.

To show: There exist σ_c, i, j such that

$\langle S[l \mapsto (d_1, \mathsf{true})]; d_1 \rangle \longrightarrow^i \sigma_c$ and $\sigma_b \longrightarrow^j \sigma_c$ 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:

  - $\langle S; \texttt{freeze } l \rangle \longrightarrow \langle S[l \mapsto (d_1, \text{true})]; d_1 \rangle$, and
  - $\langle S; \texttt{freeze } l \rangle \longrightarrow \sigma_b$.

  To show: There exist σ_c, i, j such that $\langle S[l \mapsto (d_1, \text{true})]; d_1 \rangle \longrightarrow^i \sigma_c$ and $\sigma_b \longrightarrow^j \sigma_c$ 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.

$\square$

B.10 Strong Local Quasi-Confluence

This is the proof of Lemma 2 from the main text of the paper.

Proof. By Lemma 13, either:

1. there exist i, j, π_a, π_b and σ'_c such that $\pi_a(S) = \pi_b(S) = S$ and $\pi_a(\sigma_a) \longrightarrow^i \sigma'_c$ and $\pi_b(\sigma_b) \longrightarrow^j \sigma'_c$ and $i \leq 1$ and $j \leq 1$, or

2. $\sigma_a \longrightarrow \textbf{error}$ or $\sigma_b \longrightarrow \textbf{error}$.

In the second case, we're done.
In the first case, we proceed as follows.
By renaming $\sigma_b \longrightarrow^j \pi_b^{-1}(\sigma'_c)$.
By renaming $\sigma_a \longrightarrow^j \pi_a^{-1}(\sigma'_c)$.
Choose $\pi = \pi_a^{-1} \circ \pi_b$, and $\sigma_c = \pi_b^{-1}(\sigma'_c)$.

$\square$

B.11 Strong One-Sided Quasi-Confluence

Lemma 14 (Strong One-Sided Quasi-Confluence)**.** *If $\sigma \longrightarrow \sigma'$ and $\sigma \longrightarrow^m \sigma''$, where $1 \leq m$, then either:*

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

2. *there exists $k \leq m$ such that $\sigma' \longrightarrow^k \textbf{error}$, or there exists $k \leq 1$ such that $\sigma'' \longrightarrow^k \textbf{error}$.*

Proof. We proceed by induction on m. In the base case of $m = 1$, the result is immediate from Lemma 2, with $k = 1$.
For the induction step, suppose $\sigma \longrightarrow^m \sigma'' \longrightarrow \sigma'''$ 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 π, σ_c, i, j such that $\sigma' \longrightarrow^i \sigma_c$ and $\sigma''' \longrightarrow^j \pi(\sigma_c)$ and $i \leq m + 1$ and $j \leq 1$, or

2. there exists $k \leq m + 1$ such that $\sigma' \longrightarrow^k \textbf{error}$, or there exists $k \leq 1$ such that $\sigma''' \longrightarrow^k \textbf{error}$.

From the induction hypothesis, we have that either:

1. there exist π', σ'_c, i', j' such that $\sigma' \longhookrightarrow^{i'} \sigma'_c$ and $\sigma'' \longhookrightarrow^{j'} \pi'(\sigma'_c)$ and $i' \leq m$ and $j' \leq 1$, or

2. there exists $k' \leq m$ such that $\sigma' \longhookrightarrow^{k'}$ **error**, or there exists $k' \leq 1$ such that $\sigma'' \longhookrightarrow^{k'}$ **error**.

We consider these two cases in turn:

1. There exist σ'_c, i', j' such that $\sigma' \longhookrightarrow^{i'} \sigma'_c$ and $\sigma'' \longhookrightarrow^{j'} \sigma'_c$ 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 $j = 0$ and $\pi = \pi'$.
    - If $j' = 1$:

      From $\sigma'' \longhookrightarrow \sigma'''$ and $\sigma'' \longhookrightarrow^{j'} \pi'(\sigma'_c)$ and Lemma 2, one of the following two cases is true:

      (a) There exist σ''_c and i'' and j'' such that $\pi'(\sigma'_c) \longhookrightarrow^{i''} \pi''(\sigma''_c)$ and $\sigma''' \longhookrightarrow^{j''} \sigma''_c$ and $i'' \leq 1$ and $j'' \leq 1$. So we also have $\sigma' \longhookrightarrow^{i'} \sigma'_c \longhookrightarrow^{i''} ((\pi')^{-1} \circ \pi'')\sigma''_c$. In summary, we pick $\sigma_c = \sigma''_c$ and $i = i' + i''$ and $j = j''$ and $\pi = (\pi')^{-1} \circ \pi''$, which is sufficient because $i = i' + i'' \leq m + 1$ and $j = j'' \leq 1$.

      (b) $\sigma''' \longhookrightarrow$ **error** or $\sigma'_c \longhookrightarrow$ **error**.
      If $\sigma''' \longhookrightarrow$ **error**, then choosing $k = 1$ satisfies the proof.
      Otherwise, $\sigma'_c \longhookrightarrow$ **error**, therefore $\sigma' \longhookrightarrow^{i'} \sigma'_c \longhookrightarrow$ **error**.
      Hence $\sigma' \longhookrightarrow^{i'+1}$ **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 $\sigma' \longhookrightarrow^{k'}$ **error**, or there exists $k' \leq 1$ such that $\sigma'' \longhookrightarrow^{k'}$ **error**:

    If there exists $k' \leq m$ such that $\sigma' \longhookrightarrow^{k'}$ **error**, then choosing $k = k'$ satisfies the proof.

    Otherwise, there exists $k' \leq 1$ such that $\sigma'' \longhookrightarrow^{k'}$ **error**. We proceed by cases on k':

    - If $k' = 0$, then $\sigma'' = $ **error**.
      Hence this case is not possible, since $\sigma'' \longhookrightarrow \sigma'''$ and **error** cannot step.
    - If $k' = 1$:
      From $\sigma'' \longhookrightarrow \sigma'''$ and $\sigma'' \longhookrightarrow^{k'}$ **error** and Lemma 2, one of the following two cases is true:

      (a) There exist σ''_c and i'' and j'' such that **error** $\longhookrightarrow^{i''} \sigma''_c$ and $\sigma''' \longhookrightarrow^{j''} \sigma''_c$ and $i'' \leq 1$ and $j'' \leq 1$.
      Since **error** cannot step, $i'' = 0$ and $\sigma''_c = $ **error**.
      Hence $\sigma''' \longhookrightarrow^{j''}$ **error**.
      Since $j'' \leq 1$, choosing $k = j''$ satisfies the proof.

      (b) **error** $\longhookrightarrow$ **error** or $\sigma''' \longhookrightarrow$ **error**.
      Since **error** cannot step, $\sigma''' \longhookrightarrow$ **error**.
      Hence choosing $k = 1$ satisfies the proof.

    $\square$

B.12 Strong Quasi-Confluence

Lemma 15 (Strong Quasi-Confluence). *If $\sigma \longhookrightarrow^n \sigma'$ and $\sigma \longhookrightarrow^m \sigma''$, where $1 \leq n$ and $1 \leq m$, then either:*

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

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

Proof. We proceed by induction on n. In the base case of $n = 1$, the result is immediate from Lemma 14.
For the induction step, suppose $\sigma \longhookrightarrow^n \sigma' \longhookrightarrow \sigma'''$ 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 π, σ_c, i, j such that $\sigma''' \longleftrightarrow^i \sigma_c$ and $\sigma'' \longleftrightarrow^j \pi(\sigma_c)$ and $i \leq m$ and $j \leq n+1$, or

2. there exists $k \leq m$ such that $\sigma''' \longleftrightarrow^k$ **error**, or there exists $k \leq n+1$ such that $\sigma'' \longleftrightarrow^k$ **error**.

From the induction hypothesis, we have that either:

1. there exist π', σ'_c, i', j' such that $\sigma' \longleftrightarrow^{i'} \sigma'_c$ and $\sigma'' \longleftrightarrow^{j'} \pi'(\sigma'_c)$ and $i' \leq m$ and $j' \leq n$, or

2. there exists $k' \leq m$ such that $\sigma' \longleftrightarrow^{k'}$ **error**, or there exists $k' \leq n$ such that $\sigma'' \longleftrightarrow^{k'}$ **error**.

We consider these two cases in turn:

1. There exist π', σ'_c, i', j' such that $\sigma' \longleftrightarrow^{i'} \sigma'_c$ and $\sigma'' \longleftrightarrow^{j'} \pi'(\sigma'_c)$ 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 $j = j' + 1$ and $\pi = \pi'$.

   - If $i' \geq 1$:

     From $\sigma' \longleftrightarrow \sigma'''$ and $\sigma' \longleftrightarrow^{i'} \pi'(\sigma'_c)$ and Lemma 14, one of the following two cases is true:

     (a) There exist σ''_c and i'' and j'' such that $\sigma''' \longleftrightarrow^{i''} \sigma''_c$ and $\pi'(\sigma'_c) \longleftrightarrow^{j''} \pi''(\sigma''_c)$ and $i'' \leq i'$ and $j'' \leq 1$. So we also have $\sigma'' \longleftrightarrow^{j'} \sigma'_c \longleftrightarrow^{j''} ((\pi')^{-1} \circ \pi'')(\sigma''_c)$. In summary, we pick $\sigma_c = \sigma''_c$ and $i = i''$ and $j = j' + j''$ and $\pi = (\pi')^{-1} \circ \pi''$, 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 $\sigma''' \longleftrightarrow^{k''}$ **error**, or there exists $k'' \leq 1$ such that $\sigma'_c \longleftrightarrow^{k''}$ **error**.
     If there exists $k'' \leq i'$ such that $\sigma''' \longleftrightarrow^{k''}$ **error**, then choosing $k = k''$ satisfies the proof, since $k'' \leq i' \leq m$.
     Otherwise, there exists $k'' \leq 1$ such that $\sigma'_c \longleftrightarrow^{k''}$ **error**.
     Therefore, $\sigma'' \longleftrightarrow^{j'} \sigma'_c \longleftrightarrow^{k''}$ **error**.
     Hence $\sigma'' \longleftrightarrow^{j'+k''}$ **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 $\sigma' \longleftrightarrow^{k'}$ **error**, or there exists $k' \leq n$ such that $\sigma'' \longleftrightarrow^{k'}$ **error**:

   If there exists $k' \leq n$ such that $\sigma'' \longleftrightarrow^{k'}$ **error**, then choosing $k = k'$ satisfies the proof.

   Otherwise, there exists $k' \leq m$ such that $\sigma' \longleftrightarrow^{k'}$ **error**. We proceed by cases on k':

   - If $k' = 0$, then $\sigma' = $ **error**.
     Hence this case is not possible, since $\sigma' \longleftrightarrow \sigma'''$ and **error** cannot step.

   - If $k' \geq 1$:

     From $\sigma' \longleftrightarrow \sigma'''$ and $\sigma' \longleftrightarrow^{k'}$ **error** and Lemma 14, one of the following two cases is true:

     (a) There exist σ''_c and i'' and j'' such that $\sigma''' \longleftrightarrow^{i''} \sigma''_c$ and **error** $\longleftrightarrow^{j''} \sigma''_c$ and $i'' \leq k'$ and $j'' \leq 1$.
     Since **error** cannot step, $j'' = 0$ and $\sigma''_c = $ **error**.
     Hence $\sigma''' \longleftrightarrow^{i''}$ **error**.
     Since $i'' \leq k' \leq m$, choosing $k = i''$ satisfies the proof.

     (b) There exists $k'' \leq k'$ such that $\sigma''' \longleftrightarrow^{k''}$ **error**, or there exists $k'' \leq 1$ such that **error** $\longleftrightarrow^{k''}$ **error**.
     Since **error** cannot step, there exists $k'' \leq k'$ such that $\sigma''' \longleftrightarrow^{k''}$ **error**.
     Since $k'' \leq k' \leq m$, choosing $k = k''$ satisfies the proof.

$\square$

B.13 Quasi-Confluence

Lemma 16 (Quasi-Confluence). *If $\sigma \hookrightarrow^* \sigma'$ and $\sigma \hookrightarrow^* \sigma''$, then either:*

1. *there exists π, σ_c such that $\sigma' \hookrightarrow^* \sigma_c$ and $\sigma'' \hookrightarrow^* \sigma_c$ up to a location renaming π, or*

2. $\sigma' = \text{\textbf{error}}$ *or* $\sigma'' = \text{\textbf{error}}$.

Proof. Strong Quasi-Confluence (Lemma 15) implies Quasi-Confluence. □

B.14 Quasi-Determinism

This is the proof of Theorem 1 from the main text of the paper.

Proof. By Lemma 16, one of the following two cases applies:

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

2. $\sigma' = \text{\textbf{error}}$ or $\sigma'' = \text{\textbf{error}}$, and so the result is immediate.

□

C Graph Algorithms in LVish: BFS and MIS

The recently proposed *Problem Based Benchmark Suite* [4] presents a suite of benchmark problems designed to focus on non-numerical computing on irregular problems. The PBBS release comes with high-quality parallel C++/Cilk implementations of the benchmarks. We have implemented and measured the performance of LVish versions of two of the benchmarks from this suite: *breadth-first search* (BFS) and *maximal independent set* (MIS). In addition to implementing the benchmarks themselves, we used LVish to implement a parallel parser for the ASCII graph representation format that PBBS uses. Our LVish parser implementation can parse a 557MB graph in one second on 12 cores, which is as fast as the C++ parallel parser in PBBS, *and* potentially scheduled as part of an asynchronous LVish application, rather than as a separate phase.

In short, we observe between $2.09\times$ and $2.76\times$ parallel speedup on standalone BFS (with no other handlers registered), depending on graph topology, and $1.34\times$ to $1.79\times$ parallel speedup on MIS. These problems are very fine-grained, and thus the overhead of (potentially) blocking LVish `get` operations on every vertex processed is too high for the LVish versions to be able to perform well. Yet when BFS or MIS are used to discover a part of the graph that is used as input to nontrivial per-vertex computations downstream, it becomes apparent that one advantage of using LVish is that it enables such downstream computations to start sooner, as we discuss below.

C.1 Implementation notes

The sequential implementation of MIS is straightforward. To select from a graph a maximal set of vertices that share no edges, the algorithm iterates through the vertices in order and adds a vertex to the set iff none of its already-encountered neighbors are marked for inclusion. The deterministic parallel implementation of MIS that comes with PBBS produces the same answer as the sequential version by using a mechanism called *deterministic reservations* [4]. Loop iterations are launched in parallel, but a parallel iteration will fail if the neighbor vertices of that iteration's vertex have not been processed yet, and iterations marked as having failed are then retried. The effect is exactly like that of blocking `get` in LVish; thus the LVish port of this program is elegant—identical to the sequential version with reads and writes replaced by `put` and `get`.

The bad news is that going through the LVish scheduler for *every* vertex in a graph is too heavyweight a mechanism to allow the LVish version to be competitive with the PBBS C++/Cilk implementations. In fact, the *single-core* performance of the LVish BFS implementation is $60\times$ slower than the PBBS C++/Cilk version: 0.191s compared

to 11.8s for a million-vertex grid, for example![18] ALthough the LVish BFS implementation does achieve parallel speedup, this is an untenable starting point for raw BFS performance. *However*:

- LVish should be directly compared only against other *deterministic-by-construction* models. No C++ library that executes client code in parallel can ever provide this guarantee. Of course, every implementation will have some trusted code; an LVish programmer must trust the LVish library to behave deterministically. The advantage of LVish is that the trusted computing base is of *constant size*, rather than scaling with the number of applications.

- Graph processing in LVish is more flexible than it is in the PBBS implementation: the set-based implementation handles nodes with arbitrary keys (*e.g.*, variables with call histories in k-CFA) and graphs that are discovered on the fly, rather than with a fixed, dense range of integer node IDs.

Furthermore, graph processing in LVish has certain advantages with respect to composition, latency hiding, and latency of response, as we discuss below.

C.2 Graph processing as part of a parallel pipeline

A user rarely wants to compute a property of a graph in isolation, with no meaningful node or edge labels, and no tasks to perform on those labels. Rather, graph algorithms like BFS and MIS play a role in the context of a larger application. It is in such pipeline-parallel applications that LVish is used to its best advantage, since LVish implementations of these algorithms can drive other downstream consumers asynchronously, allowing full overlap of different phases of the computation and creating the potential for latency hiding.

For example, consider a situation where the component discovered by a BFS phase is the input to a downstream task, but the graph turns out to have long linear chains. In this case, the PBBS C++/Cilk implementation has some trouble, taking 8.79s for 10 million vertices on one core (11.06s for LVish), rather than 0.191s for a graph with the same number of vertices but with a grid topology. Moreover, in the C++/Cilk implementation, the downstream task must wait for the entire BFS phase to complete. In the LVish implementation, on the other hand, the first downstream tasks execute in 0.14 to 0.23 milliseconds from the beginning of the graph traversal,[19] regardless of how many cores are used, and *even when the application is run on one core*, due to LVish's depth-first scheduling approach. This reduced latency could be important, for example, in an interactive application waiting to update the screen.

---

[18]Furthermore, these results are with an LVar type that allows atomic operations on an unboxed array; the performance for a reference `Set` LVar is worse for BFS, at 14.17s. In the future, it may make sense for LVish to provide primitive support for *bulk handling* of many blocking loop iterations, similar to deterministic reservations.

[19]This latency measurement includes the overhead launching parallel worker threads.