Abstract
We introduce Perceus, an algorithm for precise reference counting with reuse and specialization. Starting from a functional core language with explicit control-flow, Perceus emits precise reference counting instructions such that programs are garbage free, where only live references are retained. This enables further optimizations, like reuse analysis that allows for guaranteed in-place updates at runtime. This in turn enables a novel programming paradigm that we call functional but in-place (FBIP). Much like tail-call optimization enables writing loops with regular function calls, reuse analysis enables writing in-place mutating algorithms in a purely functional way. We give a novel formalization of reference counting in a linear resource calculus, and prove that Perceus is sound and garbage free. We show evidence that Perceus, as implemented in Koka, has good performance and is competitive with other state-of-the-art memory collectors.

1 Introduction
Reference counting [5], with its low memory overhead and ease of implementation, used to be a popular technique for automatic memory management. However, the field has broadly moved in favor of generational tracing collectors [28], partly due to various limitations of reference counting, including cycle collection, multi-threaded operations, and expensive in-place updates.

In this work we take a fresh look at reference counting. We consider a programming language design that gives strong compile-time guarantees in order to enable efficient reference counting at run-time. In particular, we build on the pioneering reference counting work in the Lean theorem prover [42], but we view it through the lens of language design, rather than purely as an implementation technique.

We demonstrate our approach in the Koka language [20, 22]: a functional language with mostly immutable data types together with a strong type and effect system. In contrast to the dependently typed Lean language, Koka is general-purpose, with support for exceptions, side effects, and mutable references via general algebraic effects and handlers [36, 37]. Using recent work on evidence translation [46, 47], all these control effects are compiled into an internal core language with explicit control flow. Starting from this functional core, we can statically transform the code to enable efficient reference counting at runtime. In particular:

- Due to explicit control flow, the compiler can emit precise reference counting instructions where a reference is dropped as soon as possible; we call this garbage free reference counting as only live data is retained (Section 2.2).
- We show that precise reference counting enables many optimizations, in particular drop specialization which removes many reference count operations in the fast path (Section 2.3), reuse analysis which updates (immutable) data in-place when possible (Section 2.4), and reuse specialization which removes many in-place field updates (Section 2.5). The reuse analysis shows the benefit of a holistic approach: even though the surface language has immutable data types with strong guarantees, we can use dynamic run-time information, e.g. whether a reference is unique, to update in-place when possible.
- The in-place update optimization is guaranteed, which leads to a new programming paradigm that we call FBIP: functional but in-place (Section 2.6). Just like tail-call optimization lets us write loops with regular function calls, reuse analysis lets us write in-place mutating algorithms in a purely functional way. We showcase this approach by implementing a functional version of in-order Morris tree traversal [32], which is stack-less, using in-place tree node mutation via FBIP.
- We present a formalization of general reference counting using a novel linear resource calculus, $\lambda^1$, which is closely based on linear logic (Section 3), and we prove that reference counting is sound for any program in the linear resource calculus. We then present the Perceus algorithm as a deterministic syntax-directed version of $\lambda^1$, and prove

$^1$Perceus, pronounced per-see-us, is a loose acronym of “PrEcise Reference Counting with rEUse and Specialization”.

∗The first two authors contributed equally to this work
that it is both sound (i.e. never drops a live reference), and
garbage free (i.e. only retains reachable references).
- We demonstrate Perceus by providing a full implementation
  for the strongly typed functional language Koka [1].
  The implementation supports typed algebraic effect handlers
  using evidence translation [47] and compiles into
  standard C11 code. The use of reference counting means
  no runtime system is needed and Koka programs can readily link with other C/C++ libraries.
- We show evidence that Perceus, as implemented for Koka,
  competes with other state-of-the-art memory collectors
  (Section 4). We compare our implementation in allocation
  intensive benchmarks against OCaml, Haskell, Swift,
  and Java, and for some benchmarks to C++ as well. Even
  though the current Koka compiler does not have many
  optimizations (besides the ones for reference counting), it
  has outstanding performance compared to these mature
  systems. As a highlight, on the tree insertion benchmark,
  the purely functional Koka implementation is within 10%
  of the performance of the in-place mutating algorithm
  in C++ (using std::map [10]).

Even though we focus on Koka in this paper, we believe that
Perceus, and the FBIP programming paradigm we identify,
are both broadly applicable to other programming languages
with similar static guarantees for explicit control flow.

2 Overview
Compared to a generational tracing collector, reference counting
has low memory overhead and is straightforward to implement. However, while the cost of tracing collectors
is linear in the live data, the cost of reference counting is
linear in the number of reference counting operations. Optimizing the total cost of reference counting operations is
therefore our main priority. There are at least three known
problems that make reference counting operations expensive in practice and generally inferior to tracing collectors:
- Concurrency: when multiple threads share a data structure,
  reference count operations need to be atomic, which is expensive.
- Precision: common reference counted systems are not precise
  and hold on to objects too long. This increases memory
  usage and prevents aggressive optimization of many reference
  count operations.
- Cycles: if object references form a cycle, the runtime needs
to handle them separately, which re-introduces many of
the drawbacks of a tracing collector.

We handle each of these issues in the context of an eager,
functional language using immutable data types together
with a strong type and effect system. For concurrency, we
precisely track when objects can become thread-shared (Section
2.7.2). For precision, we introduce Perceus, our algorithm
for inserting precise reference counting operations that can
be aggressively optimized. In particular, we eliminate and
fuse many reference count operations with drop specialization
(Section 2.3), turn functional matching into in-place updates with reuse analysis
(Section 2.4), and minimize field updates with reuse specialization (Section 2.5).

Finally, although we currently do not supply a cycle collector,
our design has two important mitigations. First, (co)inductive
data types and eager evaluation prevent cycles outside of
explicit mutable references, and it is statically known where
cycles can possibly be introduced in the code (Section 2.7.4).
Second, being a mostly functional language, mutable references
are not often used, and on top of that, reuse analysis greatly reduces the need for them since in-place mutation is
typically inferred.

The reference count optimizations are our main contribution
and we start with a detailed overview in the following sections, ending with details about how we mitigate the impact of concurrency and cycles.

2.1 Types and Effects
We start with a brief introduction to Koka [20, 22] – a strongly
typed, functional language that tracks all (side) effects. For example, we can define a squaring function as:

fun square( x : int ) : total int { x * x }

Here we see two types in the result: the effect type total and
the result type int. The total type signifies that the function
can be modeled semantically as a mathematically total function,
which always terminates without raising an exception
(or having any other observable side effect). Effectful
functions get more interesting effect types, like:

fun println( s : string ) : console ()
fun divide( x : int, y : int ) : exn int

where println has a console effect and divide may raise an
exception (exn) when dividing by zero. It is beyond the scope
of this paper to go into full detail, but a novel feature of Koka
is that it supports typed algebraic effect handlers which can
define new effects like async/await, iterators, or co-routines
without needing to extend the language itself [21–23].

Koka uses algebraic data types extensively. For example,
we can define a polymorphic list of elements of type a as:

type list(a) {
  Cons( head : a, tail : list(a) )
  Nil
}

We can match on a list to define a polymorphic map function
that applies a function f to each element of a list xs:

fun map( xs : list(a), f : a -> e b ) : e list(b) {
  match(xs) {
    Cons(x,xx) -> Cons(f(x), map(xx,f))
    Nil     -> Nil
  }
}

Here we transform the list of generic elements of type a to
a list of generic elements of type b. Since map itself has no
intrinsic effect, the overall effect of map is polymorphic, and
equals the effect e of the function f as it is applied to every
element. The map function demonstrates many interesting
aspects of reference counting and we use it as a running example in the following sections.

2.2 Precise Reference Counting

An important attribute that sets Perceus apart is that it is precise: an object is freed as soon as no more references remain. By contrast, common reference counting implementations tie the liveness of a reference to its lexical scope, which might retain memory longer than needed. Consider:

```typescript
fun foo() {
  val xs = list(1,1000000) // create large list
  val ys = map(xs, inc) // increment elements
  print(ys)
}
```

Many compilers emit code similar to:

```typescript
fun foo() {
  val xs = list(1,1000000)
  val ys = map(xs, inc)
  print(ys)
  drop(xs)
  drop(ys)
}
```

where we use a gray background for generated operations. The `drop(xs)` operation decrements the reference count of an object and, if it drops to zero, recursively drops all children of the object and frees its memory. These "scoped lifetime" reference counts are used by the C++ `shared_ptr` (calling the destructor at the end of the scope), Rust’s `Rc` (using the `Drop` trait), and Nim (using a `finally` block to call `destroy`) [48]. It is not required by the semantics, but Swift typically emits code like this as well [11].

Implementing reference counting this way is straightforward and integrates well with exception handling where the drop operations are performed as part of stack unwinding. But from a performance perspective, the technique is not always optimal: in the previous example, the large list `xs` is retained in memory while a new list `ys` is built. Both exist for the duration of `print`, after which a long, cascading chain of drop operations happens for each element in each list.

Perceus takes a more aggressive approach where ownership of references is passed down into each function: now `map` is in charge of freeing `xs`, and `ys` is freed by `print`: no `drop` operations are emitted inside `foo` as all local variables are consumed by other functions, while the `map` and `print` functions drop the list elements as they go. In this example, Perceus generates the code for `map` as given in Figure 1b. In the `Cons` branch, first the head and tail of the list are dupped, where a `dup(x)` operation increments the reference count of an object and returns itself. The `drop(xs)` then frees the initial list node. We need to `dup f` as well as it is used twice, while `x` and `xx` are consumed by `f` and `map` respectively.

At first blush, this seems more expensive than the scoped approach but, as we will see, this change enables many further optimizations. More importantly, transferring ownership, rather than retaining it, means we can free an object immediately when no more references remain. This both increases cache locality and decreases memory usage. For `map`, the memory usage is halved: the list `xs` is deallocated while the new list `ys` is being allocated.

2.3 Drop Specialization

Once we change to precise, ownership-based reference counting, there are many further optimization opportunities. After the initial insertion of `dup` and `drop` operations, we perform a drop specialization pass. The basic `drop` operation is defined in pseudocode as:

```typescript
fun drop(x) {
  if (is-unique(x)) then drop children of x; free(x)
  else decref(x)
}
```

and drop specialization essentially inlines the `drop` operation specialized at a specific constructor. Figure 1c shows the drop specialization of our `map` example. Note that we only apply drop specialization if the children are used, so no specialization takes place in the `Nil` branch.

Again, it appears we made things worse with extra operations in each branch, but we can perform another transformation where we push down `dup` operations into branches followed by standard `dup/drop fusion` where corresponding `dup/drop` pairs are removed. Figure 1d shows the code that is generated for our `map` example.

After this transformation, almost all reference count operations in the fast path are gone. In our example, every node in the list `xs` that we map over is unique (with a reference count of 1) and so the `if (is-unique(x))` test always succeeds, thus immediately freeing the node without any further reference counting.

2.4 Reuse Analysis

There is more we can do. Instead of freeing `xs` and immediately allocating a fresh `Cons` node, we can try to `reuse xs` directly as first described by Ullrich and de Moura [42]. Reuse analysis is performed before emitting the initial reference counting operations. It analyses each `match` branch, and tries to pair each matched pattern to allocated constructors of the same size in the branch. In our map example, `xs` is paired with the `Cons` constructor. When such pairs are found, and the matched object is not live, we generate a `drop-reuse` operation that returns a `reuse token` that we attach to any constructor paired with it:

```typescript
fun map(xs, f) {
  match(xs) {
    Cons(x,xx) {
      val ru = drop-reuse(xs)
      Cons@ru( f(x), map(xx, f))
    }
    Nil -> Nil
  }
}
```

The `Cons@ru` annotation means that (at runtime) if `ru==NULL` then the `Cons` node is allocated fresh, and otherwise the memory at `ru` is of the right size and can be used directly. Figure 1e shows the generated code after reference count insertion.
fun map( xs : list a, f : a -> e b ) : e list b {
  match(xs) {
    Cons(x,xx) -> Cons(f(x), map(xx,f))
    Nil -> Nil
  }
}

(a) A polymorphic map function

fun map( xs, f ) {
  match(xs) {
    Cons(x,xx) {
      dup(x); dup(xx);
      if (is-unique(xs))
      then drop(x); drop(xx); free(xs)
      else decref(xs);
      Cons(ru(dup(f)(x), map(xx, f)))
    }
    Nil {
      drop(xs);
      drop(f); Nil
    }
  }
}

(b) dup/drop insertion (2.2)

fun map( xs, f ) {
  match(xs) {
    Cons(x,xx) {
      if (is-unique(xs))
      then free(xs)
      else dup(x);
      dup(xx);
      decref(xs);
      Cons(ru(dup(f)(x), map(xx, f)))
    }
    Nil {
      drop(xs);
      drop(f); Nil
    }
  }
}

(c) drop specialization (2.3)

fun map( xs, f ) {
  match(xs) {
    Cons(x,xx) {
      if (is-unique(xs))
      then &xs
      else dup(x);
      dup(xx);
      Cons@ru(dup(f)(x), map(xx, f))
    }
    Nil {
      drop(xs);
      drop(f); Nil
    }
  }
}

(d) push down dup and fusion (2.3)

fun map( xs, f ) {
  match(xs) {
    Cons(x,xx) {
      val ru = if (is-unique(xs))
      then &xs
      else decref(xs);
      Cons@ru(dup(f)(x), map(xx, f))
    }
    Nil {
      drop(xs);
      drop(f); Nil
    }
  }
}

(e) reuse token insertion (2.4)

fun map( xs, f ) {
  match(xs) {
    Cons(x,xx) {
      val ru = if (is-unique(xs))
      then &xs
      else decref(xs);
      Cons@ru(dup(f)(x), map(xx, f))
    }
    Nil {
      drop(xs);
      drop(f); Nil
    }
  }
}

(f) drop-reuse specialization (2.4)

fun map( xs, f ) {
  match(xs) {
    Cons(x,xx) {
      val ru = if (is-unique(xs))
      then &xs
      else decref(xs);
      Cons@ru(dup(f)(x), map(xx, f))
    }
    Nil {
      drop(xs);
      drop(f); Nil
    }
  }
}

(g) push down dup and fusion (2.4)

Fig. 1. Drop specialization and reuse analysis for map.

Compared to the program in Figure 1b, the generated code now consumes xs using drop-reuse(xs) instead of drop(xs).

Just like with drop specialization we can also specialize drop-reuse. The drop-reuse operation is specified in pseudocode as:

```
fun drop-reuse( x ) {
  if (is-unique(x)) then drop children of x; &x
  else decref(x); NULL
}
```

where &x returns the address of x. Figure 1f shows the code for map after specializing the drop-reuse. Again, we can push down and fuse the dup operations, which finally results in the code shown in Figure 1g. In the fast path, where xs is uniquely owned, there are no more reference counting operations at all! Furthermore, the memory of xs is directly reused to provide the memory for the Cons node for the returned list – effectively updating the list in-place.

### 2.5 Reuse Specialization

The final transformation we apply is reuse specialization, by which we can further reuse unchanged fields of a constructor. A constructor expression like Cons@ru(x, xx) is implemented in pseudocode as:

```
fun Cons@ru( x, xx ) {
  if (ru!=NULL)
    then { ru->head := x; ru->tail := xx; ru } // in-place
  else Cons(x,xx) // malloc'd
}
```

However, for our map example there would be no benefit to specializing as all fields are assigned. Thus, we only specialize constructors if at least one of the fields stays the same. As an example, we consider insertion into a red-black tree [14].

We define red-black trees as:

```
type color { Red; Black }
type tree {
  Leaf
  Node(color: color, left: tree, key: int, value: bool, right: tree)
}
```

The red-black tree has the invariant that the number of black nodes from the root to any of the leaves is the same, and that a red node is never a parent of red node. Together this ensures that the trees are always balanced. When inserting nodes, the invariants need to be maintained by rebalancing the nodes when needed. Okasaki’s algorithm [34] implements this elegantly and functionally (the full algorithm can be found in Appendix A):

```
fun bal-left( l : tree, k : int, v : bool, r : tree ): tree {
  match(l) {
    Node(_, Node(Red, lx, kx, vx, rx), ky, vy, ry)
      -> Node(Leaf(Red, lx, k, v, ry))
    ...
  }
}
```

```
fun ins( t : tree, k : int, v : bool ): tree {
  match(t) {
    Leaf -> Node(Red, Leaf, k, v, Leaf)
    Node(Red, l, kx, vx, rx), ky, vy, ry)
  }
}
Fig. 2. Morris in-order tree traversal algorithm in C.

```c
void inorder( tree* root, void (*f)(tree* t) ) {
  tree* cursor = root;
  while (cursor != NULL /* Tip */) {
    if (cursor->left == NULL) {
      // no left tree, go down the right
      f(cursor->value);
      cursor = cursor->right;
    } else (
      // has a left tree
      tree* pre = cursor->left; // find the predecessor
      while(pre->right != NULL && pre->right != cursor) {
        pre = pre->right;
      }
      if (pre->right == NULL) {
        // first visit, remember to visit right tree
        pre = cursor; // 재할당
        cursor = cursor->left;
      } else (
        // already set, restore
        f(cursor->value);
        pre->right = NULL; // 재할당
        cursor = cursor->right;
      }
    } // end while
  }
}
```

Fig. 3. FBIP in-order tree traversal algorithm in Koka.

For this kind of program, reuse specialization is effective. For example, if we look at the second branch in `ins` we see that the newly allocated `Node` has almost all of the same fields as `t` except for the left tree `l` which becomes `ins(l,k,v)`. After reuse specialization, this branch becomes:

```koka
tmap( f : int -> int, t : tree, d : direction ) : tree {
  match(d) {
    Up -> tmap(f,Up,t) // A
    Down -> tmap(f,Down,t) // B
    Done -> t // C
  }
  fun tmap( t : tree, f : int -> int ) : tree {
    type direction { Up; Down; }
    type visitor {
      Done;
      BinR( right:tree, value : int, visit : visitor )
      BinL( left:tree, value : int, visit : visitor )
    }
    if (match(t) == Up) {
      tmap(f,tmap(t,f),Up) // C
    } else {
      f(tmap(f,t,map(Up),Down)) // B
    }
}
```

In the fast path, where `t` is uniquely owned, `t` is reused directly, and only its left child is re-assigned as all other fields stay unchanged. This applies to many branches in this example and saves many assignments.

Moreover, the compiler inlines the `bal-left` function. At that point, every matched `Node` constructor has a corresponding `Node` allocation – if we consider all branches we can see that we either match one `Node` and allocate one, or we match three nodes deep and allocate three. With reuse analysis this means that every `Node` is reused in the fast path without doing any allocations!

Essentially this means that for a unique tree, the purely functional algorithm above adapts at runtime to an in-place mutating re-balancing algorithm (without any further allocation). Moreover, if we use the tree `persistently` [33], and the tree is shared or has shared parts, the algorithm adapts to copying exactly the shared spine of the tree (and no more), while still rebalancing in place for any unshared parts.

2.6 A New Paradigm: Functional but In-Place (FBIP)

The previous red-black tree rebalancing showed that with Perceus we can write algorithms that dynamically adapt to use in-place mutation when possible (and use copying when used persistently). Importantly, a programmer can rely on this optimization happening, e.g. they can see the `match` patterns and match them to constructors in each branch.

This style of programming leads to a new paradigm that we call FBIP: “functional but in place”. Just like tail-call optimization lets us describe loops in terms of regular function calls, reuse analysis lets us describe in-place mutating imperative algorithms in a purely functional way (and get persistence as well). Consider mapping a function `f` over all elements in a binary tree in-order:

```koka
tmap( f : int -> int, t : tree ) {
  fun tmap( t : tree, f : int -> int ) : tree {
    if (t == Tip) {
      return Tip;
    } else {
      return tmap(f,tmap(t,f),Down) // B
    }
  }
  tmap(f,tmap(Tip,f),Up) // A
}
```

This is already quite efficient as all the `Bin` and `Tip` nodes are reused in-place when `t` is unique. However, the `tmap` function is not tail-recursive and thus uses as much stack space as the depth of the tree.

In 1968, Knuth posed the problem of visiting a tree in-order while using no extra stack- or heap space [19] (For readers not familiar with the problem it might be fun to try this in your favorite imperative language first and see that it is not easy to do). Since then, numerous solutions have appeared in the literature. A particularly elegant solution was proposed by Morris [32]. This is an in-place mutating algorithm that swaps pointers in the tree to “remember” which parts are unvisited. It is beyond this paper to give a full explanation, but a C implementation is shown in Figure 2. The traversal essentially uses a right-threaded tree to keep track of which nodes to visit. The algorithm is subtle, though.
Since it transforms the tree into an intermediate graph, we need to state invariants over the so-called Morris loops [26] to prove its correctness.

We can derive a functional and more intuitive solution using the FBIP technique. We start by defining an explicit visitor data structure that keeps track of which parts of the tree we still need to visit. In Koka we define this data type as visitor given in Figure 3. (Interestingly, our visitor data type can be generically derived as a list of the derivative of the tree data type\(^2\) [17, 27]). We also keep track of which direction we are going, either Up or Down the tree.

We start our traversal by going downward into the tree with an empty visitor, expressed as \(\text{map}(f, t, \text{Done}, \text{Down})\). The key idea is that we are either Done (C), or, on going downward in a left spine we remember all the right trees we still need to visit in a BinR (A) or, going upward again (B), we remember the left tree that we just constructed as a BinL while visiting right trees (O). When we come back (E), we restore the original tree with the result values. Note that we apply the function \(f\) to the saved value in branch O (as we visit in-order), but the functional implementation makes it easy to specify a pre-order traversal by applying \(f\) in branch A, or a post-order traversal by applying \(f\) in branch E.

Looking at each branch we can see that each Bin matches up with a BinR, each BinR with a BinL, and finally each BinL with a Bin. Since they all have the same size, if the tree is unique, each branch updates the tree nodes in-place at runtime without any allocation, where the visitor structure is effectively overlaid over the tree nodes while traversing the tree. Since all map calls are tail calls, this also compiles to a loop and thus needs no extra stack- or heap space.

Finally, just like with re-balancing tree insertion, the algorithm as specified is still purely functional: it uses in-place updating when a unique tree is passed, but it also adapts gracefully to the persistent case where the input tree is shared, or where parts of the input tree are shared, making a single copy of those parts of the tree.

2.7 Static Guarantees and Language Features

So far we have shown that precise reference counting enables powerful analyses and optimizations of the reference counting operations. In this section, we use Koka as an example to discuss how strong static guarantees at compile-time can further allow the precise reference counting approach to be integrated with non-trivial language features.

2.7.1 Non-Linear Control Flow. An essential requirement of our approach is that programs have explicit control flow so that it is possible to statically determine where to insert \(\text{dup}\) and \(\text{drop}\) operations. However, it is in tension with functions that have non-linear control flow, e.g. may throw an exception, use a \texttt{longjmp}, or create an asynchronous continuation that is never resumed. For example, if we look at the code for \texttt{map} before applying optimizations, we have:

\[
\text{fun map}(\, x, f \, ) \{ \\
\quad \text{match}(x) \{ \\
\quad\quad \text{Ok}(y) \rightarrow \{ \text{match}(\text{map}(x, f)) \{ \\
\quad\quad\quad \text{Error}(\text{err}) \rightarrow \{ \text{drop}(y); \text{Error}(\text{err}) \} \\
\quad\quad\quad \text{Ok}(y) \rightarrow \{ \text{match}(\text{map}(x, f)) \{ \\
\quad\quad\quad\quad \text{Error}(\text{err}) \rightarrow \text{drop}(y); \text{Error}(\text{err}) \\
\quad\quad\quad\quad \text{Ok}(y) \rightarrow \text{Cons}(y, y) \} \\
\quad\quad\quad \} \\
\quad\quad \text{Error}(\text{err}) \rightarrow \{ \text{drop}(y); \text{Error}(\text{err}) \} \\
\quad\quad \text{Ok}(y) \rightarrow \text{Cons}(y, y) \} \\
\quad\text{Err}(\text{err}) \rightarrow \{ \text{drop}(y); \text{Err}(\text{err}) \} \\
\quad\text{Ok}(y) \rightarrow \text{Cons}(y, y) \} \\
\} \\
\}\]

At this point all errors are explicitly propagated and all control-flow is explicit again. Note the we have no reference count operations on the \texttt{error} values as these are implemented as \texttt{value} types which are not heap allocated. This is similar to error handling in Swift [18] (although it requires the programmer to insert a \texttt{try} at every invocation), and also similar to various C++ proposals [40] where exceptions become explicit error values.

The example here is specialized for exceptions but the actual Koka implementation uses a generalized version of this technique to implement a multi-prompt delimited control monad [15] instead, which is used in combination with evidence translation [47] to express general algebraic effect handlers (which in turn subsume all other control effects, like exceptions, async/await, probabilistic programming, etc).

\(^2\)Conor McBride [27] describes how we can generically derive a \texttt{zipper} [17] visitor for any recursive type \(\mu x.F\) as a list of the derivative of that type, namely \(\mu x.\mu y.F\mid\mu y.x\). In our case, calculating the derivative of the inductive tree, we get \(\mu x.1 + (\text{tree} \times \text{int} \times x) + (\text{tree} \times \text{int} \times x)\), which corresponds to the visitor datatype.

\(^3\)Koka actually generalizes this using a multi-prompt delimited control monad that works for any control effect, with essentially the same principle.
2.7.2 Concurrent Execution. If multiple threads share a reference to a value, the reference count needs to be incremented and decremented using atomic operations which can be expensive. Ungar et al. [43] report slowdowns up to 50% when atomic reference counting operations are used. Nevertheless, in languages with unrestricted multi-threading, like Swift, almost all reference count operations need to assume that references are potentially thread-shared.

In Koka, the strong type system gives us additional guarantees about which variables may need atomic reference count operations. Following the solution of Ullrich and de Moura [42], we mark each object with whether it can be thread-shared or not, and supply an internal polymorphic operation 

\[
tshare : \forall a. a \to \text{io} ()
\]

that references are potentially thread-shared.

In Koka, the strong type system gives us additional guarantees about which variables may need atomic reference count operations. Following the solution of Ullrich and de Moura [42], we mark each object with whether it can be thread-shared or not, and supply an internal polymorphic operation 

\[
tshare : \forall a. a \to \text{io} ()
\]

that references are potentially thread-shared.

The read operation \(!\) first reads the current reference in \(x\), and then increments its reference count. Suppose though that before the \(\text{dup}\), the thread is suspended and another thread writes to the same reference: it will read the same object into \(y\), update the reference, and then drop \(y\) — and if \(y\) has a reference count of 1 it will be freed! When the other thread resumes, it will now try to \(\text{dup}\) the just-freed object.

To make this work correctly, we need to perform both operations atomically, either through a double-CAS [6], using hazard pointers [12, 30], or using some other locking mechanism. Either way, this can be quite expensive. Fortunately, in our setting, we can avoid the slow path in most cases. First of all, since FBIP allows for the efficiency of in-place updates with a purely functional specification (Section 2.6), we expect mutable references to be a last resort rather than the default. Secondly, as discussed in Section 2.7.2, we can also check if a mutable reference is actually thread-shared and thus avoid the atomic code path almost all of the time. In other settings though mutability can be costly; for example in Swift objects are mutable and behave like a mutable reference cell when most fields can be updated in-place, and therefore many field accesses need to be treated just like mutable reference cell operations. Moreover, as discussed in the previous section as well, the compiler must assume most of the time that objects might be thread-shared and thus use the slow atomic code path [43].

2.7.3 Mutation. Mutation in Koka is done through explicit mutable references. Here we look at first-class mutable reference cells, but Koka also has second-class mutable local variables that can be more convenient. A mutable reference cell is created with \(\text{ref}\), dereferenced with \(!\) and updated using \(:=\):

\[
\begin{align*}
\text{fun } \text{ref} (\text{init : a}) & : \text{st(h)} \text{ref(h,a)} \\
\text{fun } (!) (r : \text{ref(h,a)}) & : \text{st(h) a} \\
\text{fun } (:=)(r : \text{ref(h,a)}, x : a) & : \text{st(h) x}
\end{align*}
\]

where each operation has a stateful effect \(\text{st(h)}\) in some heap \(h\). A reference cell of type \(\text{ref(h,a)}\) is a first-class value that contains a reference to a value of type \(a\). As such, there are always two reference counts involved: that of the reference itself, and that of value that is referenced.

When a mutable reference cell is thread-shared, this presents a problem as an update operation may \textit{race} with a read operation to update the reference counts. The pseudocode implementation of both operations is:

\[
\begin{align*}
\text{fun } (!) (r) & \{ \\
\text{val } x = r->\text{value} \quad \text{val } y = r->\text{value} \\
\text{dup}(x) \quad \text{r->value := x} \\
\text{drop } y & \}
\end{align*}
\]

The read operation \(!\) first reads the current reference in \(x\), and then increments its reference count. Suppose though that before the \(\text{dup}\), the thread is suspended and another thread writes to the same reference: it will read the same object into \(y\), update the reference, and then drop \(y\) — and if \(y\) has a reference count of 1 it will be freed! When the other thread resumes, it will now try to \(\text{dup}\) the just-freed object.

To make this work correctly, we need to perform both operations atomically, either through a double-CAS [6], using hazard pointers [12, 30], or using some other locking mechanism. Either way, this can be quite expensive. Fortunately, in our setting, we can avoid the slow path in most cases. First of all, since FBIP allows for the efficiency of in-place updates with a purely functional specification (Section 2.6), we expect mutable references to be a last resort rather than the default. Secondly, as discussed in Section 2.7.2, we can also check if a mutable reference is actually thread-shared and thus avoid the atomic code path almost all of the time. In other settings though mutability can be costly; for example in Swift objects are mutable and behave like a mutable reference cell when most fields can be updated in-place, and therefore many field accesses need to be treated just like mutable reference cell operations. Moreover, as discussed in the previous section as well, the compiler must assume most of the time that objects might be thread-shared and thus use the slow atomic code path [43].

2.7.4 Cycles. A known limitation of reference counting is that it cannot release cyclic data structures. Just like with mutability, we try to mitigate its performance impact by reducing the potential for this to occur in the first place. In Koka, almost all data types are immutable and either \textit{inductive} or \textit{coinductive}. It can be shown that such data types are never cyclic (and functions that recurse over such data types always terminate).
In practice, mutable references are the main way to construct cyclic data. Since mutable references are uncommon in our setting, we leave the responsibility to the programmer to break cycles by explicitly clearing a reference cell that may be part of a cycle. Since this strategy is also used by Swift, a widely used language where most object fields are mutable, we believe this is a reasonable approach to take for now. However, we have plans for future improvements: since we know statically that only mutable references are able to form a cycle, we could generate code that tracks those data types at run time and may perform a more efficient form of incremental cycle collection.

2.7.5 Summary. In summary, we have shown how static guarantees at compile-time can be used to mitigate the performance impact of concurrency and the risk of cycles. This paper does not yet present a general solution to all problems with reference counting and future work is required to explore how cycles can be handled more efficiently, and how well Perceus can be used with implicit control flow. Yet, we expect that our approach gives new insights in the variables of a pattern

$$\lambda$$

expression $e$ borrowed environment given a $e$ an expression multisets. For example, $(\ )$ use the compact comma notation for summing (or splitting) drop are not exposed to users. Among those constructs, $\text{dup}$ match $\text{val}$ explicit binding as $\text{Figure 4}$ defines the syntax of our linear resource calculus

3 A Linear Resource Calculus

In this section we present a novel linear resource calculus, $\lambda$, which is closely based on linear logic. The operational semantics of $\lambda$ is formalized in an explicit heap with reference counting, and we prove that the operational semantics is sound. We then formalize Perceus as a sound and precise syntax-directed algorithm of $\lambda$ and thus provide a theoretic foundation for Perceus.

3.1 Syntax

Figure 4 defines the syntax of our linear resource calculus $\lambda$. It is essentially an untyped lambda calculus extended with explicit binding as $\text{val} x = e_1; e_2$, and pattern matching as match. We assume all patterns in match are mutually exclusive, and all pattern binders are distinct. Syntactic constructs in gray are only generated in derivations of the calculus and are not exposed to users. Among those constructs, dup and drop form the basic instructions of reference counting.

Contexts $\Delta, \Gamma$ are multisets containing variable names. We use the compact comma notation for summing (or splitting) multisets. For example, $(\Gamma, x)$ adds $x$ to $\Gamma$, and $(\Gamma_1, \Gamma_2)$ appends two multisets $\Gamma_1$ and $\Gamma_2$. The set of free variables of an expression $e$ is denoted by $\text{fv}(e)$, and the set of bound variables of a pattern $p$ by $\text{bv}(p)$.

3.2 The Linear Resource Calculus

The derivation $\Delta \mid \Gamma \vdash e \rightarrow e'$ in Figure 5 reads as follows: given a borrowed environment $\Delta$, a linear environment $\Gamma$, an expression $e$ is translated into an expression $e'$ with explicit reference counting instructions. We call variables in the linear environment owned.

The key idea of $\lambda$ is that each resource (i.e., owned variable) is consumed exactly once. That is, a resource needs to be explicitly duplicated (in rule $\text{dup}$) if it is needed more than once; or be explicitly dropped (in rule $\text{drop}$) if it is not needed. The rules are closely related to linear typing.

Following the key idea, the variable rule $\text{var}$ consumes a resource when we own and only own $x$ exactly once in the owned environment. For example, to derive the K combinator, $\lambda x \ y \ . \ x$, we need to apply $\text{drop}$ to be able to discard $y$, which gives $\lambda x \ . \ \text{drop} \ y \ ; \ x$.

The $\text{app}$ rule splits the owned environment $\Gamma$ into two separate contexts $\Gamma_1$ and $\Gamma_2$ for expression $e_1$ and $e_2$ respectively. Each expression then consumes its corresponding owned environment. Since $\Gamma_2$ is consumed in the $e_2$ derivation, we know that resources in $\Gamma_2$ are surely alive when deriving $e_1$, and thus we can borrow $\Gamma_2$ in the $e_1$ derivation. The rule is quite similar to the [$\text{let!]}$ rule of Wadler’s linear type rules [44,p.14] where a linear type can be “borrowed” as a regular type during evaluation of a binding.

Borrowing is important as it allows us to conduct a dup as late as possible, or otherwise we will need to duplicate enough resources before we can divide the owned environment. Consider $\lambda f \ g \ . \ (f \ x) \ (g \ x)$. Without borrowing, we have to duplicate $x$ before the application, resulting
applied, so it is derived under an empty borrowed environment only owning the argument and the free variables (in the closure). The translated lambda is also annotated with \( y s \), as \( \lambda^y x . e \), so we know precisely the resources the lambda should own when evaluated in a heap semantics. We often omit the annotation when it is irrelevant.

The \texttt{bind} rule is similar to application and borrows \( \Gamma_2 \) in the derivation for the bound expression. This is the main reason to not consider \( \text{val} \ x = e_1 ; e_2 \) as syntactic sugar for \( (\lambda x . e_1) e_2 \). The \texttt{match} rule consumes the scrutinee and owns the bound variables in each pattern for each branch. For constructors (rule \texttt{con}), we divide the owned environment into \( n \) parts for each component, and allow each component derivation to borrow the owned environment of the components derived later.

We use the notation \( \lbrack e \rbrack \) to erase all drop and dup in the expression \( e \). We can now state that derivations leave expressions unchanged except for inserting dup/drop operations:

\[ \text{if } \Delta \vdash \Gamma \vdash e \sim e' \text{ then } e = \lbrack e \rbrack. \]

\textbf{Lemma 1.} (Translation only inserts dup/drop)

If \( \Delta \vdash \Gamma \vdash e \sim e' \) then \( e = \lbrack e \rbrack \).

\section{3.3 Semantics}

Figure 6 defines standard semantics for \( \lambda^l \) using strict evaluation contexts \cite{ground}. The evaluation contexts uniquely determine where to apply an evaluation step. As such, evaluation contexts neatly abstract from the usual implementation context of a stack and program counter. Rule \texttt{(match)} replays on the internal form of expression \texttt{match} \( e \{ p_i \mapsto e'_i \} \); after substitution (\texttt{(app)}), values may appear in positions where only variables were allowed, and this is exactly what enables us to do pattern match on a data constructor.

In Figure 7 we define our target semantics of a reference counted heap, so sharing of values becomes explicit and substitution only substitutes variables. Here, each heap entry \( x \mapsto v \) points to a value \( v \) with a reference count of \( n \) (with \( n \geq 1 \)). In these semantics, values other than variables are allocated in the heap with rule \texttt{(lam)}, and rule \texttt{(con)}.

The evaluation rules discard entries from the heap when the reference count drops to zero. Any allocated lambda is annotated as \( \lambda^y x . e \) to clarify that these are essentially \texttt{closures} holding an environment \( y s \) and a code pointer \( \lambda x . e \). Note that it is important that the environment \( y s \) is a multi-set. After the initial translation, \( y s \) will be equivalent to the free variables in the body (see rule \texttt{lam}), but during evaluation substitution may substitute several variables with the same reference. To keep reference counts correct, we need to keep considering each one as a separate entry in the closure environment.

When applying an abstraction, rule \texttt{(app)} needs to satisfy the assumptions made when deriving the abstraction in rule \texttt{lam}. First, the \texttt{(app)} rule inserts dup to duplicate variables \( y s \), as these are owned in rule \texttt{lam}. It then drops the reference to the closure itself. Rule \texttt{(match)} is similar to
We say a variable $y$ is reachable in terms of a heap $H$ and an expression $e$, denoted as $\text{reach}(x, H \mid e)$, if (1) $x \in \text{fv}(e)$; or (2) for some $y$, we have $\text{reach}(y, H \mid e) \land y \mapsto^n v \in H \land \text{reach}(x, H \mid v)$.

To prove this theorem we need to maintain strong invariants at each evaluation step to ensure a variable is still alive if it is going to be referred later. The proof can be found in Appendix D.2. Second, we prove that the reference counting semantics never hold on to unused variables. We first define the notion of reachability.

**Definition 1.** (Reachability) We say a variable $x$ is reachable in terms of a heap $H$ and an expression $e$, denoted as $\text{reach}(x, H \mid e)$, if (1) $x \in \text{fv}(e)$; or (2) for some $y$, we have $\text{reach}(y, H \mid e) \land y \mapsto^n v \in H \land \text{reach}(x, H \mid v)$.

With reachability, we can formally show:

**Theorem 2.** (Reference counting leaves no garbage) Given $\emptyset \vdash e \rightarrow e'$ and $\emptyset \vdash e' \rightarrow^* e'', H \mid x$, then for every intermediate state $H_i \mid e_i$, we have that for all $y \in \text{dom}(H_i)$, $\text{reach}(y, H_i \mid e_i)$.

In Appendix D.3, we further show that the reference counts are exactly equal to the number of actual references to the resource. Notably, to capture the essence of precise reference counting, $\lambda^1$ does not model mutable references (Section 2.7.3). From Theorem 2 we see that mutable references are indeed the only source of cycles. A natural extension of the system is to include mutable references and thus cycles. In that case, we could generalize Theorem 2, where the conclusion would be that for all resource in the heap, it is either reachable from the expression, or it is part of a cycle.

The above theorems establish the correctness of the reference-counted heap semantics. However, correctness does not imply precision, i.e. that the heap is garbage free. Eventually all live data is discarded but it may well hold on to live data too long by delaying drop operations. As an example, consider $\emptyset \vdash e \rightarrow^1 (\lambda x. x) \rightarrow^\ast e \rightarrow^1 (\lambda x. x) \rightarrow^\ast y$ where $y$ is reachable but dropped too late: it is only dropped after the lambda gets allocated. In contrast, a garbage free algorithm would produce $y \rightarrow^1 (\lambda x. x) \rightarrow^\ast y \rightarrow^1 (\lambda x. x) \rightarrow^\ast y$. In the next section we present Perceus as a syntax directed algorithm of the linear resource calculus and show that it is garbage free.

### 3.4 Perceus

Figure 8 defines syntax directed derivation $\tau_s$ for our resource calculus and as such specifies our Perceus algorithm. Like before, $\Delta \mid \Gamma \vdash_e e \rightarrow e'$ translates an expression $e$ to $e'$ under an borrowed environment $\Delta$ and an owned environment $\Gamma$. During the derivation, we maintain the following invariants: (1) $\Delta \cap \Gamma = \emptyset$; (2) $\Gamma \subseteq \text{fv}(e)$; (3) $\text{fv}(e) \subseteq \Delta, \Gamma$; and (4) multiplicity of each member in $\Delta, \Gamma$ is 1. We ensure these properties hold by construction at any step in a derivation.
\[\Delta \mid \Gamma \vdash x \rightsquigarrow x \quad \Delta \cap \Gamma = \emptyset \quad \Gamma \subseteq \text{fv}(e) \quad \text{fv}(e) \subseteq \Delta, \Gamma \quad \text{multiplicity of each member in } \Delta, \Gamma \text{ is 1}\]

\[
\Delta, x \mid t_3 \vdash x \rightsquigarrow x \quad \text{[svar]} \\
\Delta, \Delta_2 \mid t_2 \vdash e_1 \rightsquigarrow e_1' \quad \Delta \cap \Gamma \vdash e_2 \rightsquigarrow e_2' \quad \Delta_2 = \Gamma \cap \text{fv}(e_2) \quad \text{[sapp]} \\
\frac{x \in \text{fv}(e) \quad \Delta, \Delta_1 \mid s \vdash \text{dup} \Delta_1 \vdash \lambda^{y_x} x. e \rightsquigarrow e'}{\Delta, \Delta_1 \mid \Gamma \vdash x \rightsquigarrow \text{dup} \Delta_1 \vdash \lambda^{y_x} x. e \rightsquigarrow e'} \quad \text{[slam-drop]} \\
\frac{x \notin \text{fv}(e_2) \quad \Delta, \Gamma \mid s \vdash e \rightsquigarrow e'}{\Delta, \Delta_1 \mid s \vdash e \rightsquigarrow e'} \quad \text{[sbind-drop]} \\
\frac{x \notin \text{fv}(e_2) \quad \Delta, \Gamma \mid s \vdash e \rightsquigarrow e'}{\Delta, \Delta_1 \mid s \vdash e \rightsquigarrow e'} \quad \text{[smatch]} \\
\frac{\Delta, \Gamma \vdash x \rightsquigarrow \text{match } \{ p_i \mapsto e_i \} \rightsquigarrow \text{match } \{ p_i \mapsto \text{drop } \Delta_i' \vdash e_i' \} \quad \text{[scon]}}{\Delta, \Gamma \vdash C \; \text{v}_1 \ldots \text{v}_n \rightsquigarrow C \; \text{v}_1' \ldots \text{v}_n'} \]

Fig. 8. Syntax-directed linear resource rules of \(\lambda^l\).

The Perceus rules are set up to do precise reference counting: we delay a dup operation to come as late as possible, pushing them out to the leaves of a derivation; and we generate a drop operation as soon as possible, right after a binding or at the start of a branch.

Rule svar-dup borrows \(x\) by inserting a dup. The sapp rule now deterministically finds a good split of the environment \(\Gamma\). We pass the intersection of \(\Gamma\) with the free variables in \(e_2\) to the \(e_2\) derivation. Otherwise the rule is the same as in the declarative system. For abstraction and binding we have two variants: one where the binding is actually in the free variables of the expression (rule slam and sbind), and one where the binding can be immediately dropped as it is unused (rule slam-drop and sbind-drop). In the abstraction rule, we know that \(\Gamma \subseteq \text{fv}(\lambda x. e)\) and thus \(\Gamma \sqsubseteq y_s\). If there are any free variables not in \(\Gamma\), they must be part of the borrowed environment (as \(\Delta_1\)) and these must be duplicated to ensure ownership. The bind rules are similarly constructed as a mixture of sapp and slam.

The smatch rule is interesting as in each branch there may be variables that can be dropped as they no longer occur as free variables in that branch. The owned environment \(\Gamma_i\) in the \(i\)th branch is the intersection of \((\Gamma, \text{bv}(p_i))\) and the free variables in that branch; any other owned variables (as \(\Gamma'_i\)) are dropped at the start of the branch. Rule scon deterministically splits the environment \(\Gamma\) as in rule sapp.

We show that the Perceus algorithm is sound by showing that for each rule there exists a derivation in the declarative linear resource calculus. The proof is given in Appendix D.4.

**Theorem 3.** (Syntax directed translation is sound)
If \(\Delta \mid \Gamma \vdash e \rightsquigarrow e'\) then also \(\Delta \mid \Gamma \vdash e \rightsquigarrow e'\).

More importantly, we prove that any translation resulting from the Perceus algorithm is precise, where any intermediate state in the evaluation is garbage free (Appendix D.5):

**Theorem 4.** (Perceus is precise and garbage free)
If \(\emptyset \mid \emptyset \vdash e \rightsquigarrow e'\) and \(\emptyset \mid e \rightsquigarrow e'\), then for every intermediate state \(H \mid e\), \(e\) is not a dup/drop operation \((e_i \neq \text{E[drop } x; e'_i\) and \(e_i \neq \text{E[drop } x; e'_i\)) we have that for all \(y \in \text{dom}(H), \text{reach}\; (y, H; \mid [e_i])\).

This theorem states that after evaluating any immediate reference counting instructions, every variable in the heap is reachable from the erased expression. This rules out, for example, \(y \mapsto 1 \) (\(\lambda x. x\) (drop \(y; (i)\)) as \(y\) is not in the free variables of the erased expression. Just like Theorem 2, if the system is extended with mutable references, then Theorem 4 could be generalized such that every resource is either reachable from the erased expression, or it is part of a cycle.

The implementation of Perceus is further extended with the optimizations described in Section 2. As the component transformations, including inlining and dup/drop fusion, are standard, the soundness of those optimizations follows naturally and a proof is beyond the scope of this paper.
We also run Koka “no-opt” with reuse analysis and drop/reuse specialization disabled to measure the impact of those optimizations.

- OCaml 4.08.1. This has a stop-the-world generational collector with a minor and major heap. The minor heap uses a copying collector, while a tracing collector is used for the major heap [8, 31, Chap. 22]. The Koka benchmarks correspond essentially one-to-one to the OCaml versions.

- Haskell, GHC 8.6.5. A highly optimizing compiler with a multi generational garbage collector. The benchmark sources again correspond very closely, but since Haskell has lazy semantics, we used strictness annotations in the data structures to speed up the benchmarks, as well as to ensure that the same amount of work is done.

- Swift 5.3. The only other language in this comparison where the compiler uses reference counting [4, 43]. The benchmarks are directly translated to Swift in a functional style without using direct mutation. However, we translated tail-recursive definitions to explicit loops with local variables.

- Java SE 15.0.1. Uses the HotSpot JVM and the G1 concurrent, low-latency, generational garbage collector. The benchmarks are directly translated from Swift.

- C++, gcc 9.3.0. A highly optimizing compiler with manual memory management. Without automatic memory management, many benchmarks are difficult to express directly in C++ as they use persistent and partially shared data structures. To implement these faithfully would essentially require manual reference counting. Instead, we use C++ as our performance baseline: if provided, we either use in-place updates without supporting persistence (as in rbtree which uses std::map) or we do not reclaim memory at all (as in deriv, nqueens, and cfold).

The benchmarks are all chosen to be medium sized and nontrivial, and all stress memory allocation with little computation. Most of these are based on the benchmark suite of Lean [42] and all are available in the Koka repository [1]. The execution times and peak working set averaged over 10 runs and normalized to Koka are given in Figure 9. When a benchmark is not available for a particular language, it is marked as × in the figures.

- rbtree: inserts 42 million items into a red-black tree.

- rbtree-ck: a variant of rbtree that keeps a list of every 5th subtree and thus shares many subtrees.

- deriv: the symbolic derivative of a large expression.

- nqueens: calculates all solutions for the n-queens problem of size 13 into a list, and returns the length of that list. The solution lists share many sub-solutions.

- cfold: constant-folding over a large symbolic expression.

We can see from Figure 9 that even though Koka has few optimizations besides the reference counting ones, it performs very well compared to these mature systems, often outperforming by a significant margin – both in execution time and peak working set. We only discuss the overall results...
here, but appendix B includes a detailed discussion of each individual benchmark.

In the rbtree benchmark, the functional implementation of Koka is within 10% of the highly optimized, in-place updating, std::map implementation in C++. We believe this is partly because C++ allocations must be 16-byte aligned while the Koka allocator can use 8-byte alignment and thus allocate a bit less. The rbtree benchmark also shows the potential effectiveness of the reference count optimizations where the "no-opt" version is more than 2× slower. However, in benchmarks with lots of sharing, like deriv and nqueens, the optimizations are less effective.

Since Perceus is garbage free we would expect that Koka always uses less memory than a GC based system. This is indeed the case in our benchmarks – except for OCaml in deriv. Through manual inspection of OCaml’s machine code, we believe that OCaml avoids some allocations by applying "case of case" transformations [35] which are not (yet) available in the Koka compiler.

5 Related Work

Our work is closely based on the reference counting algorithm in the Lean theorem prover as described by Ullrich and de Moura [42]. They describe reuse analysis based on reset/reuse instructions, and describe both reference counting based on ownership (i.e. precise) but also support borrowed parameters. We extend their work with drop- and reuse specialization, and generalize to a general purpose language with side-effects and complex control flow. We also introduce a novel formalization of reference counting with the linear resource calculus, and define our algorithm in terms of that. As such, the Perceus algorithm may differ from the Lean one as that is specified over a lower-level calculus that uses explicit partial application nodes (pap) and has no first-class lambda expressions.

Schulte [39] describes an algorithm for inserting reference count instructions in a small first-order language and shows a limited form of reuse analysis, called “reusage” (transformation T14).

Using explicit reference count instructions in order to optimize them via static analysis is described as early as Barth [2]. Mutating unique references in place has traditionally focused on array updates [16], as in functional array languages like Sisal [29] and SaC [13, 38]. Férey and Shankar [9] provide functional array primitives that use in-place mutation if the array has a unique reference; we plan to add these to Koka.

We believe this would work especially well in combination with reuse-analysis for BTree-like structures using trees of small functional arrays.

The λ₁ calculus is closely based on linear logic. The main difference is that, in systems with linear types (e.g., Wandler [44]), the linear (or uniqueness) property is static whereas reference counts track this dynamically. Turner and Wandler [41] give a heap-based operational interpretation which does not need reference counts as linearity is tracked by the type system. In contrast, Chirimar et al. [3] give an interpretation of linear logic in terms of reference counting, but in their system, values with a linear type are not guaranteed to have a unique reference at runtime.

The Swift language is widely used in iOS development and uses reference counting with an explicit representation in its intermediate language. There is no reuse analysis but, as remarked by Ullrich and de Moura [42], this may not be so important for Swift as typical programs mutate objects in-place. There is no cycle collection for Swift, but despite the widespread usage of mutation this seems to be not a large problem in practice. Since it can be easy to create accidental cycles through the self pointer in callbacks, Swift has good support for weak references to break such cycles in a declarative manner.

Swift uses reference counting with an explicit representation in its intermediate language. Ungar et al. [43] optimize atomic reference counts by tagging objects that can be potentially thread-shared. Later work by Choi et al. [4], uses biased reference counting to avoid many atomic updates.

Another recent language that uses reference counting is Nim. The reference counting method is scope-based and uses non-atomic operations (and objects cannot be shared across threads without extra precautions). Nim can be configured to use ORC reference counting which extends the basic ARC collector with a cycle collection [48]. Nim has the acyclic annotation to identify data types that are (co)-inductive, as well as the (unsafe) cursor annotation for variables that should not be reference counted.

In our work we focus on precise and garbage free reference counting which enables static optimization of reference count instructions. On the other extreme, Deutsch and Bobrow [7] consider deferred reference counting – any reference count operations on stack-based local variables are deferred and only the reference counts of fields in the heap are maintained. Much like a tracing collector, the stack roots are periodically scanned and deferred reference counting operations are performed. Levanoni and Petrank [25] extend this work and present a high performance reference counting collector for Java that uses the sliding view algorithm to avoid many intermediate reference counting operations and needs no synchronization on the write barrier.

6 Conclusion

In this paper we present Perceus, a precise reference counting system with reuse and specialization, which is built upon λ₁, a novel linear resource calculus closely based on linear logic. Our full implementation in Koka is competitive with other mature memory collectors. In future work, we would like to study ways to handle cycles efficiently. Moreover, we would like to integrate selective “borrowing” into Perceus – this would make certain programs no longer be garbage...
We like to thank Erez Petrank for the discussions on the race conditions that can occur with in-place updates and reference counts.

7 Acknowledgements

We like to thank Erez Petrank for the discussions on the race conditions that can occur with in-place updates and reference counts.

References


Appendix

A  Red-black tree implementation

Figure 10 shows balanced insertion into a red-black tree using Okasaki’s algorithm [34].

B  Extended Benchmark Discussion

Here we discuss the results of each individual benchmark from Figure 9 in more detail:

- rbtree: this performs 42 million insertions into a red-black balanced tree and after that folds over the tree counting the true elements. Here the reuse analysis of Koka shines (as shown in Section 2.4) and it outperforms all other systems where only OCaml is close in performance – rebalancing generates lots of short-lived object allocation which are a great fit for the minor heap copying-collector of OCaml with fast aggregated bump-pointer allocation. The C++ benchmark is implemented using the in-place updating std::map implementation, which internally uses a highly optimized red-black tree implementation [10]. Surprisingly, the purely functional Koka implementation is within 10% of the C++ performance. Since the insertion operations are the same, we believe this is partly because C++ allocations must be 16-byte aligned while the Koka allocator can use 8-byte alignment in the allocations and thus allocate a bit less (as apparent in Figure 9) (and similarly, bump pointer allocation in OCaml can be faster than general malloc/free). Java performs close to C++ here but also uses almost 10× the memory of Koka (1.7GiB vs. 170MiB, Figure 9). This can be reduced to about 1.5× by providing tuning parameters on the command line but that also made it slower on our system. The effects of the reuse analysis and specialization optimizations can also be significant with optimized Koka being more than twice as fast as "no-opt".

- rbtree-ck: in previous reviews, it has been suggested that rbtree is biased to reference counting as it has no shared subtrees and thus reuse analysis can use in-place updates all the time. The rbtree-ck benchmark remedies this and is a variant of rbtree that keeps a list of every 5th tree generated and thus shares many subtrees. Again, Koka outperforms all other systems. Haskell and OCaml are now relatively slower than in rbtree – we conjecture this is due to extra copying between generations, and perhaps due to increased tracing cost.

- deriv: calculates the derivative of a large symbolic expression. Again, Koka does very well here. Interestingly, the memory usage of OCaml is slightly less than Koka – since Perceus is garbage free we would expect that Koka always uses less memory than a GC based system. From studying the generated code of OCaml we believe that it is because the optimizing OCaml compiler can avoid some allocations by applying "case of case" transformations [35] which the

def type color {
    Red
    Black
}

def type tree {
    Leaf
    Node(color: color, left: tree, key: int, value: bool, right: tree)
}

def fun is-red(t: tree): bool {
    match(t) {
        Node(Red) -> True
        _ -> False
    }
}

def fun bal-left(l: tree, k: int, v: bool, r: tree): tree {
    match(l) {
        Leaf -> Leaf
        Node(_, Node(_, l, k, v, r), ky, vy, ry) ->
            Node(Node(Black, l, k, v, lx), ky, vy, ry)
        Node(_, ly, ky, vy, Node(Red, lx, kx, vx, rx)) ->
            Node(Red, Node(Black, ly, k, v, ly), ky, vy, ry)
        Node(_, lx, kx, vx, rx) ->
            Node(Black, Node(Red, lx, kx, vx, rx), k, v, r)
    }
}

def fun bal-right(l: tree, k: int, v: bool, r: tree): tree {
    match(r) {
        Leaf -> Leaf
        Node(_, Node(_, l, k, v, r), ky, vy, ry) ->
            Node(Node(Black, l, k, v, lx), k, v, ry)
        Node(_, lx, kx, vx, Node(Red, rx, k, v, ry)) ->
            Node(Red, Node(Black, lx, kx, vx, rx), k, v, ry)
        Node(_, lx, kx, vx, rx) ->
            Node(Black, l, k, v, Node(Red, lx, kx, vx, rx))
    }
}

def fun ins(t: tree, k: int, v: bool): tree {
    match(t) {
        Leaf -> Node(Red, Leaf, k, v, Leaf)
        Node(Red, l, k, v, r) -> if (k < kx) then Node(Red, ins(l, k, v), kx, vx, r)
         else Node(Black, ins(l, k, v), kx, vx, r)
        _ -> t
    }
}

def fun set-black(t: tree): tree {
    match(t) {
        Node(_, l, k, v, r) -> Node(Black, l, k, v, r)
        _ -> t
    }
}

def fun insert(t: tree, k: int, v: bool): tree {
    if (is-red(t))
        then set-black(ins(t, k, v))
    else ins(t, k, v)
}

Fig. 10. Red-black tree balanced insertion in Koka

naive Koka compiler is not (yet) doing. It is also interesting to see that the "no-opt" Koka is only a bit slower than
optimized Koka here. This is probably due to the sharing of many sub-expressions when calculating the derivative. This in turn causes the code resulting from drop/reuse specialization and reuse analysis to mostly use the “slow” path which is equivalent to the one in “no-opt”. Finally, Java performs best on this benchmark; we can see while running the benchmark that it can run the G1 collector fully concurrently on another core.

- **nqueens**: calculates all solutions for the n-queens problem of size 13 into a list, and returns the length of that list. The solution lists share many sub-solutions and, as in deriv, for the C++ version we do not free any memory (but do allocate the same objects as the other benchmarks). Again, Koka is quite competitive even with the large amount of shared structures, and the peak working set is significantly lower.

- **cfold**: performs constant-folding over a large symbolic expression. This benchmark is similar to the deriv benchmark and manipulates a complex expression graph. Koka does significantly better than other systems. Just as in deriv, we see that OCaml uses slightly less memory as it can avoid some allocations by optimizing well. The “no-opt” version of Koka also uses 8% less memory; this is because the reuse analysis essentially holds on to memory for later reuse. Just like with scoped based reference counting that may lead to increased memory usage in some situations.

An interesting overall observation is that the reference counting implementation of Swift is not doing as well as Koka – this may be partly due to the language and compiler, but we also believe that this is a confirmation of our initial hypothesis where we argue that a combination of static compiler optimizations with dynamic runtime checks (e.g. is-unique) are needed for best results. As discussed for example in Section 2.7.2, some of the optimizations we perform are difficult to do in Swift as the static guarantees of the language are not strong enough.

## C Further Benchmarks

Figure 11 show execution time and peak working sets on a 10-core Intel Core i9-7900X at 4.30GHz, Ubuntu 20.04.

Figure 12 show execution time and peak working sets on a 16-core AMD 5950X at 3.4Ghz.
Fig. 12. Relative execution time and peak working set with respect to Koka (lower is better). On a 16-core AMD 5950X at 3.4Ghz, Ubuntu 20.04.
D Proofs

D.1 A Heap Reference Counting Calculus

\[ \frac{H \vdash v \vdash H_1 \ldots H_{n-1} \vdash v_n \vdash H_n}{H \vdash C \vdash v \ldots v_n \vdash H_n} \text{ [DRCON]} \]

\[ \frac{H, x \mapsto v + x \vdash H, x \mapsto v}{H, x \mapsto v + x \vdash H, x \mapsto v} \text{ [DRVAR]} \]

\[ \frac{H, x \mapsto y \vdash H_1}{H, x \mapsto y \vdash H_1} \text{ [DRVARLAM]} \]

\[ \frac{H, x \mapsto C \vdash H_1}{H, x \mapsto C \vdash H_1} \text{ [DRVARCON]} \]

\[ \frac{H, x \mapsto v \vdash e + H_1}{H, x \mapsto v \vdash e + H_1} \text{ [DRDUP]} \]

\[ \frac{H, x \mapsto v \vdash e + H_1}{H, x \mapsto v \vdash e + H_1} \text{ [DRDROP]} \]

\[ \frac{H, x \mapsto \text{drop } ys \vdash e + H_1}{H, x \mapsto \text{drop } ys \vdash e + H_1} \text{ [DRDROPCON]} \]

\[ \frac{H, x \mapsto \text{drop } ys \vdash e + H_1}{H, x \mapsto \text{drop } ys \vdash e + H_1} \text{ [DRDROPLAM]} \]

\[ \frac{H \vdash ys \vdash H_1}{H \vdash ys \vdash H_1} \text{ [DRLAM]} \]

\[ \frac{H \vdash e \vdash H_1}{H \vdash e \vdash H_1} \text{ [DRAPP]} \]

\[ \frac{H \vdash e_1 \vdash H_1, H_1 \vdash e_2 \vdash H_2}{H \vdash e_1 \vdash e_2 \vdash H_2} \text{ [DRBIND]} \]

\[ \frac{H \vdash x \vdash H_1, H_1 \vdash \text{val } x = e_1; e_2 \vdash H_2}{H \vdash x \vdash H_1, H_1 \vdash \text{val } x = e_1; e_2 \vdash H_2} \text{ [DRMATCH]} \]

**Lemma 2. (Heap Reference Counting Free variables)**
If \( H_1 \vdash e \vdash H_2 \), then \( \text{fv}(e) \in H_1 \), and \( \text{fv}(H_2) \in H_1 \) with same domains.

**Proof. (Of Lemma 2)** By a straightforward induction on the rules. \( \square \)

**Definition 2. (Extension)**
H is extended with x, denoted as \( H \hat{=} x \), where \( \hat{=} \) works as follows:
1. if \( H = H' \), \( x \mapsto v \vdash H' \), then \( H \hat{=} x \vdash H' \), \( x \mapsto v \vdash H' \);
2. if \( x \not\in H \), then \( H \hat{=} x \vdash H \hat{=} x \vdash H' \).

We omit the domain of x in \( H \hat{=} x \) for simplicity. The domain should always be available by inspecting the heap (in (1)) or via explicit passing (in (2)).
We only focus on situations where there is no cycles in the dependency of \( x \) (but we are fine with existing cycles in \( H \)), so that the extension terminates. That implies \((H, x \mapsto^1 v) \leftrightarrow \text{fv}(v) = H \uplus \text{fv}(v), x \mapsto^1 v \) in (2).

**Lemma 3. (Drop is dual to extension)**

If \( H \uplus \text{drop} x; () \vdash H_2 \), then \( H_1 = H_2 \uplus x \). Similarly, if \( H \vdash x \uplus H_2 \), then \( H_1 = H_2 \uplus x \).

**Proof. (Of Lemma 3)** By induction on the judgment.

**case**

\[
H, x \mapsto^{n+1} ys \vdash \text{drop} x; () \vdash H, x \mapsto^n ys \tag{DRDROP, DRCON}
\]

**case**

\[
H, x \mapsto^1 \lambda y z. e \vdash \text{drop} x; () \vdash H_1 \tag{DRDROPALAM}
\]

\[
H = H_1 \uplus ys \tag{I.H.}
\]

\[
H, x \mapsto^1 \lambda y z. e = H_1 \uplus x \tag{by definition}
\]

\[
\square
\]

**Lemma 4. (Extension is dual to drop)**

\( H \uplus x \vdash \text{drop} x; () \vdash H \). Similarly, \( H \uplus x \vdash x \uplus H \).

**Proof. (Of Lemma 4)** By induction on \( \uplus x \).

**case**

\[
H = H', x \mapsto^n ys \tag{if}
\]

\[
H \uplus x = H', x \mapsto^{n+1} ys \tag{by definition}
\]

\[
H', x \mapsto^{n+1} ys \vdash \text{drop} x; () \vdash H \tag{DRDROP}
\]

**case**

\[
x \notin H \tag{if}
\]

\[
ys = \text{fv}(v) \tag{let}
\]

\[
H \uplus x = H \uplus ys, x \mapsto^1 v \tag{by definition}
\]

\[
H \uplus ys \vdash ys \uplus H \tag{I.H.}
\]

\[
H \uplus ys, x \mapsto^1 v \vdash x \uplus H \tag{DRVRLAM or DRVARCON}
\]

\[
\square
\]

**Lemma 5. (Extension Commutativity)**

\( H \uplus x \uplus y = H \uplus y \uplus x \).

**Proof. (Of Lemma 5)** By induction on \( \uplus x \) and \( \uplus y \), then we do case analysis. **case**\( x \in H \). Then \( H = H', x \mapsto^n v. \) By definition, \( H \uplus x \uplus y = (H', x \mapsto^{n+1} v) \uplus y. \) Since the way \( \uplus \) works only depends on whether \( x \) exists but not the exact number of its occurrence, we can decrease the number of \( x \), do \( \uplus y \) and then add \( x \) back. That is, \((H', x \mapsto^{n+1} v) \uplus y = (H', x \mapsto^n v) \uplus y \uplus x = H \uplus y \uplus x. \)

**case**\( y \in H \) is similar as the previous case.

**case** \( x, y \notin H. \) Then \( H \uplus x = H \uplus xs, x \mapsto^1 v \) where \( xs = \text{fv}(v) \).

**subcase** Assume \( \uplus y \) won’t cause \( \uplus x \), then \( \uplus y \) doesn’t care about the existence of \( x. \)

So \((H \uplus xs, x \mapsto^1 v) \uplus y = H \uplus xs \uplus y, x \mapsto^1 v = H \uplus y \uplus xs, x \mapsto^1 v \) by I.H.

\[
= H \uplus y \uplus x \tag{by definition}
\]
subcase Or otherwise \( \# y \) will cause \( \# x \). Since there is no cycle in the dependency, that means \( \# x \) won't cause \( \# y \). Then we can prove it as in the previous case.  □

D.1.1 Relating to linear resource calculus.

**Definition 3.** (Context to Dependency Heap)

Given a context \( \Gamma \), \( [\Gamma] \) defines a dependency heap, with all \( x \) becoming \( x \mapsto n \) if \( x \) appears \( n \) times in \( \Gamma \).

**Lemma 6.**

\( [\Gamma, x] \vdash x \mapsto [\Gamma] \). Similarly, if \( [\Delta] \vdash e \mapsto H \), then \( [\Gamma, x] \vdash \text{drop } x; e \vdash \text{H} \).

**Proof.** The goal holds by rule \text{drvar} (\text{drdrop}) when \( x \in \Gamma \) or by rule \text{drvarcon} (\text{drdropcon}) if \( x \notin \Gamma \). □

**Lemma 7.** (linear resource calculus relates to reference counting)

If \( \Delta \vdash e \mapsto e' \), then \( [\Delta, \Gamma] \vdash e' \mapsto [\Gamma] \).

**Proof.** (Of Lemma 7) By induction on the elaboration.

\[\begin{align*}
\text{case } & \Delta | x \vdash x \mapsto x \quad \text{given} \\
& [\Delta, x] \vdash x \mapsto [\Delta] \quad \text{Lemma 6} \\
\text{case } & \Delta | \Gamma \vdash e \mapsto \text{dup } x; e' \quad \text{given} \\
& \Delta | \Gamma, x \vdash e \mapsto e' \quad \text{given} \\
& x \in \Delta, \Gamma \quad \text{given} \\
& [\Delta, \Gamma, x] \vdash e' \mapsto [\Delta] \quad \text{I.H.} \\
& [\Delta, \Gamma] \vdash \text{dup } x; e' \mapsto [\Delta] \quad \text{drdup} \\
\text{case } & \Delta | \Gamma, x \vdash e \mapsto \text{drop } x; e' \quad \text{given} \\
& \Delta | \Gamma \vdash e \mapsto e' \quad \text{given} \\
& [\Delta, \Gamma, x] \vdash e' \mapsto [\Delta] \quad \text{I.H.} \\
& [\Delta, \Gamma, x] \vdash \text{drop } x; e' \mapsto [\Delta] \quad \text{Lemma 6} \\
\text{case } & \Delta | \Gamma \vdash \lambda x. e \mapsto \lambda y^{y s} x. e' \quad \text{given} \\
& \emptyset \vdash y^{y s}, x \vdash e \mapsto e' \quad \text{given} \\
& y^{y s} = \text{fv}(\lambda x. e) \quad \text{given} \\
& [\Delta, y^{y s}] \vdash y^{y s} \mapsto [\Delta] \quad \text{Lemma 6} \\
& [y^{y s}, x] \vdash e' \mapsto \emptyset \quad \text{I.H.} \\
& [\Delta, y^{y s}] \vdash \lambda y^{y s} x. e \mapsto [\Delta] \quad \text{drlam} \\
\text{case } & \Delta | \Gamma, \Gamma_1 \vdash e_1 e_2 \mapsto e'_1 e'_2 \quad \text{given} \\
& \Delta | \Gamma, \Gamma_2 \vdash e_1 \mapsto e'_1 \quad \text{given} \\
& [\Delta, \Gamma, \Gamma_1, \Gamma_2] \vdash e'_1 \mapsto [\Delta, \Gamma_2] \quad \text{I.H.} \\
& [\Delta, \Gamma, \Gamma_1, \Gamma_2] \vdash e'_2 \mapsto [\Delta] \quad \text{I.H.} \\
& [\Delta, \Gamma, \Gamma_1, \Gamma_2] \vdash e'_1 e'_2 \mapsto [\Delta] \quad \text{drapp} \\
\end{align*}\]
\[ \begin{align*} 
\Delta \vdash \Gamma, x \vdash \text{match } x \{ p_i \mapsto e_i \} & \leadsto \text{match } x \{ p_i \mapsto e_i' \} & \text{given} \\
\Delta \vdash \Gamma, \text{bv}(p_i) \vdash e_i & \mapsto e_i' & \text{given} \\
[\Delta, \Gamma, x] & \vdash x + [\Delta, \Gamma] & \text{Lemma 6} \\
[\Delta, \Gamma] & \vdash \text{match } x \{ p_i \mapsto e_i' \} + [\Delta] & \text{dmatch} \\
\Delta \vdash \Gamma_1, \ldots, \Gamma_n \vdash C \; v_1 \ldots v_n & \leadsto C \; v'_1 \ldots v'_n & \text{given} \\
\Delta, \Gamma_{i+1}, \ldots, \Gamma_n \vdash \Gamma_i \vdash v_i & \text{given} \\
[\Delta, \Gamma_i, \Gamma_{i+1}, \ldots, \Gamma_n] & \vdash v_i - [\Delta, \Gamma_{i+1}, \ldots, \Gamma_n] & \text{I.H.} \\
[\Delta, \Gamma_1, \ldots, \Gamma_n] & \vdash C \; v_1 \ldots v_n + [\Delta] & \text{drcon} \\
\end{align*} \]

\[ \square \]

### D.1.2 Weakening.

**Lemma 8. (Weakening)**

If \( H_1 \vdash e \vdash H_2 \), then \( H_1 \vdash x \vdash e \vdash H_2 \vdash x \).

**Proof. (Of Lemma 8)** By induction on the judgment.

case

\[ \begin{align*} 
H & \vdash C \; v_1 \ldots v_n - \vdash H_n & \text{given} \\
H & \vdash v_i \vdash H_i & \text{drcon} \\
H \vdash x \vdash v_i \vdash H_1 \vdash x & \text{I.H.} \\
H \vdash C \; v_1 \ldots v_n \vdash H_1 \vdash x & \text{drcon} \\
\end{align*} \]

case

\[ \begin{align*} 
H & \vdash y \vdash H_2 & \text{given} \\
H & = H_2 \vdash y & \text{Lemma 3} \\
H & \vdash x \vdash H_2 \vdash y \vdash x & \text{Lemma 5} \\
H & \vdash x \vdash y \vdash x \vdash H_2 \vdash x & \text{Lemma 4} \\
\end{align*} \]

case

\[ \begin{align*} 
H, y \vdash^n \; ys \vdash \text{dup } y; e \vdash H_1 & \text{given} \\
H, y \vdash^{n+1} \; ys \vdash e \vdash H_1 & \text{droup} \\
(H, y \vdash^n \; ys) \; \# y \vdash e \vdash H_1 & \text{definition of } \# \\
(H, y \vdash^n \; ys) \; \# y \vdash x \vdash e \vdash H_1 \vdash x & \text{I.H.} \\
(H, y \vdash^n \; ys) \; \# y \vdash x & \text{Lemma 5} \\
(H, y \vdash^n \; ys) \; \# x \vdash y \vdash e \vdash H_1 \vdash x & \text{By substitution} \\
(H, y \vdash^n \; ys) \; \# x \vdash \text{dup } y; e \vdash H_1 \vdash x & \text{droup} \\
\end{align*} \]

case
\[ H \vdash \text{drop } y; \ e \vdash H_2 \quad \text{given} \]
\[ H \vdash \text{drop } y; \ () \vdash H_3 \quad \text{follows} \]
\[ H_3 \vdash e \vdash H_2 \quad \text{above} \]
\[ H = H_3 \vdash y \quad \text{Lemma 3} \]
\[ H \vdash x = H_3 \vdash y \vdash x \]
\[ = H_3 \vdash x \vdash y \quad \text{Lemma 5} \]
\[ H_3 \vdash x \vdash y \vdash \text{drop } y; \ () \vdash H_3 \vdash x \]
\[ H_3 \vdash x \vdash e \vdash H_2 \vdash x \quad \text{I.H.} \]
\[ H_3 \vdash x \vdash \text{drop } y; \ e \vdash H_2 \vdash x \quad \text{Follows} \]
\[ H \vdash x \vdash \text{drop } y; \ e \vdash H_2 \vdash x \quad \text{By substitution} \]

\[ \text{case} \]
\[ H \vdash \lambda z. e \vdash H_1 \quad \text{given} \]
\[ H \vdash ys \vdash H_1 \quad \text{given} \]
\[ ys \mapsto_{1} (,) \vdash e \vdash \varnothing \quad \text{given} \]
\[ H \vdash x \vdash ys \vdash H_1 \vdash x \quad \text{L.H.} \]
\[ H \vdash x \vdash \lambda z. e \vdash H_1 \vdash x \quad \text{drlam} \]

\[ \text{case} \]
\[ H \vdash e_1 e_2 \vdash H_2 \quad \text{given} \]
\[ H \vdash e_1 \vdash H_1 \quad \text{given} \]
\[ H_1 \vdash e_2 \vdash H_2 \quad \text{given} \]
\[ H \vdash x \vdash e_1 \vdash H_1 \vdash x \quad \text{I.H.} \]
\[ H_1 \vdash x \vdash e_2 \vdash H_2 \vdash x \quad \text{I.H.} \]
\[ H \vdash x \vdash e_1 e_2 \vdash H_2 \vdash x \quad \text{drapp} \]

\[ \text{case} \]
\[ H \vdash \text{val } z = e_1 : e_2 \vdash H_2 \quad \text{given} \]
\[ H \vdash e_1 \vdash H_1 \quad \text{given} \]
\[ H_1, z \mapsto_{1} (,) \vdash e_2 \vdash H_2 \quad \text{given} \]
\[ z \notin H \quad \text{given} \]
\[ H \vdash x \vdash e_1 \vdash H_1 \vdash x \quad \text{I.H.} \]
\[ (H_1, z \mapsto_{1} (,) \vdash x \vdash e_2 \vdash H_2 \vdash x) \quad \text{I.H.} \]
\[ z \notin H_1 \quad \text{Lemma 2} \]
\[ H_1, z \mapsto_{1} (,) = H_1 \vdash z \]
\[ (H_1, z \mapsto_{1} (,) \vdash x = H_1 \vdash z \vdash x) \quad \text{Lemma 5} \]
\[ = H_1 \vdash x \vdash z \]
\[ = H_1 \vdash x, z \mapsto_{1} (,) \]
\[ H \vdash x \vdash e_1 e_2 \vdash H_2 \vdash x \quad \text{by substitution} \]

\[ \text{case} \]
H † match z { \( \frac{p_i \mapsto e_i}{\cdot} \) } + H’  
  (given)

H † z \vdash H_1  
  (given)

H_1, H_i † e_i \vdash H’  
  (given)

H_i = \{ [bv(p_i)] \}  
  (given)

H † x † z \vdash H_1 \vdash x  
  (LH.)

(H_1, H_2) \vdash x \vdash e_i \vdash H’ \vdash x  
  (LH.)

bv(p_i) fresh  
  (assume)

H_1, [H_i] = H_1 \vdash bv(p_i)  
  (Lemma 5)

(H_1, H_i) \vdash x = H_1 \vdash bv(p_i) \vdash x  
= H_1 : x \vdash bv(p_i)  
  (Lemma 5)

H_1 \vdash x, H_i \vdash e_i \vdash H’ \vdash x  
  (by substitution)

H † x † match z { \( \frac{p_i \mapsto e_i}{\cdot} \) } \vdash H’ \vdash x  
  (drmatch)

\( \square \)

D.2 Soundness of Reference Counting Semantics

Lemma 9. (Reference counting semantics is sound (small step))

If \( e_1 \rightarrow e_2 \), and \( H_1 \) ok, and \( e_1’ \) ok, and \( [H_1] e_1’ = e_1 \), and \( H_1 \vdash e_1’ \vdash H’_1 \), then there exists \( H_2, e_2’ \) such that \( H_1 \vdash e_1’ \mapsto^*_{r} H_2 \vdash e_2’ \), and \( [H_2] e_2’ = e_2 \).

Proof. (Of Lemma 9) By induction on the evaluation judgment.

case (app) \( (\lambda x. e) \; v \rightarrow e'[x:=v] \)

\[ [H_1] e_1’ = (\lambda x. e) \; v \]  
  (given)

subcase \( e_1’ = f \; z \).

\[ [H_1](f \; z) = (\lambda x. e) \; v \]  
  (given)

\[ [H_1] f = (\lambda x. e) \]  
  (follows)

\[ [H_1] z = v \]  
  (follows)

\( f \mapsto^n \lambda y \cdot s. \; e’ \in H_1 \)  
  (above)

\[ [H_1] e’ = e \]  
  (follows)

\( H_1 \vdash f \; z \mapsto^r H_1 \mid dup \; y \; s. \; drop \; f \; ; \; e’[x:=z] \)  
  (app)

\[ H_1 \vdash f \; z \mid H’_1 \]  
  (given)

\[ H_1 = H’_1 \vdash f \neg z \]  
  (Lemma 3)

\[ H_1 \vdash ok \]  
  (given)

\[ ys \in H_1 \]  
  (f \mapsto^n \lambda y \cdot s. \; e’ \in H_1)

\[ H_1 \mid dup \; y \; s. \; drop \; f \; ; \; e’[x:=z] \]  
  (dup and +)

\( \rightarrow_r H_1 \vdash ys \mid drop \; f \; ; \; e’[x:=z] \)  
  (Lemma 5)

\( H_1 \vdash ys = H’_1 \vdash f \neg z + ys \)  
  (Lemma 4)

\( H_1 \vdash ys \mid drop \; f \; ; \; e’[x:=z] \)  
  (Lemma 14)

\( H_1 \vdash ys \neg z + e’[x:=z] \mid H’_1 \)  
  (Lemma 2)

\[ f (e’[x:=z]) \in H_1 \neg y \; s \; z + \neg z \]  
  (known)

\[ ys \in H_1 \]  
  (known)

\[ f (e’[x:=z]) \in H_1 \]  
  (known)

\[ [H’_1 \vdash ys \neg z + e’[x:=z]] (e’[x:=z]) \]  
  (known)

\[ [H_1] (e’[x:=z]) \]  
  (by substitution)

\[ [H_1][e’][x:=[H_1]] z \]  
  (by substitution)

\[ e[x:=v] \]

subcase \( e_1’ = (\lambda x. e’) \; z \)
\[ \text{[H]} \]((\lambda x. e') z) = (\lambda x. e) v \quad \text{given} \\
[H] e' = e \quad \text{follows} \\
[H] z = v \quad \text{follows} \\
H | (\lambda x. e') z \mapsto H, f \mapsto \lambda y x. e' | f z \quad \text{(lam) and step} \\
f \text{fresh, } y s = f v(\lambda x. e') \quad \text{above} \\
H, f \mapsto \lambda y x. e' \quad \text{above} \\
f z \quad \text{ok} \quad \text{above} \\
[H, f \mapsto \lambda y x. e'](f z) = (\lambda x. e v) \quad \text{by substitution} \\
\] 

subcase The rest subcases are \( e' = f v' \) and \( e' = (\lambda x. e') v' \) where \( v' \) is not a variable. Both cases are similar as the previous one, with values stored in the heap first and the expression being \( f z \) as in the first subcase.

case \( \text{(match) match } (C v_1 \ldots v_n) \{ p_i \mapsto e_i \} \mapsto e_i[x_1 \ldots x_n=v_n] \) with \( p_i = C x_1 \ldots x_n \).

\[ H[H] e_i' = \text{match } (C v_1 \ldots v_n) \{ p_i \mapsto e_i \} \quad \text{given} \\
[H] x = C v_1 \ldots v_n \quad \text{above} \\
[H] e_i' = e_i \quad \text{above} \\
x \mapsto^n C y_1 \ldots y_n \in H_1 \quad \text{follows} \\
[H] y_i = v_i, \ldots, [H] y_n = v_n \quad \text{above} \\
H | \text{match } x \{ p_i \mapsto e_i' \} \mapsto, H_1 \quad \text{dup } y s ; \text{ drop } x ; e_i'[x s:=y s] \quad \text{(match)} \\
p_i = C x s \\
H_1 \mapsto \text{match } x \{ p_i \mapsto e_i' \} + H_1' \quad \text{given} \\
H_1 \mapsto x \mapsto H_2 \quad \text{drmatch} \\
H_2, [[x s]] \mapsto e_i + H' \quad \text{above} \\
H_1 = H_2 \mapsto x \quad \text{Lemma 3} \\
H_1 \mapsto \text{dup } y s ; \text{ drop } x ; e_i[x s:=y s] \\
H_1 \mapsto y s = H_2 \mapsto x + y s \quad \text{(dup) and \#} \\
= H_2 \mapsto y s + x \quad \text{known} \\
H_1 \mapsto y s \mapsto H_2 \mapsto y s \quad \text{Lemma 5} \\
\text{H_1 and H_2 \# y s differs only in x} \\
H_2 \mapsto y s \mapsto e_i[x s:=y s] + H_1' \quad \text{Lemma 15} \\
f v(e_i[x s:=y s]) \in H_2 \mapsto y s \\
[H_2 \mapsto y s \{ e_i[x s:=y s] \} = [H_1 \{ e_i[x s:=y s] \}] \\
([H_1] e_i)(x s:=y s) \quad \text{by substitution} \\
(e_i)[x s:=y s] \\
\text{case (dup) dup x; e \mapsto e} \\
[H] e_i' = \text{dup x; e } \quad \text{given} \\
e_i' = \text{dup x; e}' \quad \text{follows} \\
[H] e' = e \quad \text{above} \\
H_1 \mapsto \text{dup x; e}' + H_1' \quad \text{given} \\
x \in H_1 \quad \text{follows} \\
H_1 \mapsto \text{dup x; e}' + H_1 \quad \text{(dup) and \#} \\
[H] e' = [H_1] e' = e \quad \text{known} \\
\text{case (drop) drop x; e \mapsto e}
Lemma 10. (Reference counting semantics is sound (big step, part 1))

Given \( E[e_1], \) and \( H_1 \), and \( e'_1 \), and \([H_1]e'_1 = E[e_1]\), and \( H_1 \vdash e'_1 \vdash H'_1 \), then there exists \( H_2, E'' \) and \( e'_2 \) such that \( H_1 \models e'_1 \rightarrow_r^* H_2 \mid E'[e'_2] \), and \([H_2]E' = E \), and \([H_2]e'_2 = e_1\).

Proof. (Of Lemma 10) By induction on the evaluation context \( E \).

1. **case** \( E = \square \). Let \( E' = \square \) and \( e'_1 = e'_1 \), then the goals follow trivially.

2. **case** \( E = E_1 e \).

   \[ [H_1]e'_1 = E_1[e_1] e \quad \text{given} \]
   \[ e'_1 = e'_2 e'_3 \quad \text{for some } e'_2, e'_3 \]
   \[ [H_1]e'_2 = E_1[e_1] \quad \text{follows} \]
   \[ [H_1]e'_3 = e \quad \text{follows} \]
   \[ H_1 \vdash e'_2 e'_3 + H'_1 \quad \text{given} \]
   \[ H_1 \vdash e'_2 + H_3 \quad \text{DRAPP} \]
   \[ H_3 \vdash e'_3 + H'_1 \quad \text{above} \]
   \[ H_1 \vdash e'_2 \rightarrow_r^* H_2 \mid E'[e'_2] \quad \text{LH.} \]
   \[ [H_2]E' = E_1 \quad \text{above} \]
   \[ [H_2]e'_2 = e_1 \quad \text{above} \]
   \[ E'' = E'[e'_2] \quad \text{let} \]
   \[ H_1 \vdash e'_2 e'_3 \rightarrow_r^* H_2 \mid E'[e'_2] e'_3 \quad \text{step} \]
   \[ H_1 \vdash E'[e'_2] e'_3 + H'_1 \quad \text{by substitution} \]
   \[ H_2 \vdash E'[e'_2] e'_3 + H'_1 \quad \text{Lemma 15} \]
   \[ \text{fv}(e'_2) \in H_2 \quad \text{Lemma 2} \]

   \[ [H_2]E' = [H_2]E' [H_2]e'_3 \]
   \[ = [H_2]E' [H_1]e'_3 \]
   \[ = E_1 e \]

   **case** \( E = x E_1 \).
\[ [H_1]e'_1 = x \ E_1[e_1] \]
\[ e'_1 = y \ e'_3 \]
\[ [H_1]y = x \]
\[ [H_1]e'_3 = E_1[e_1] \]
\[ H_1 \vdash y \ e'_3 + H'_1 \]
\[ H_1 \vdash y \ l H_3 \]
\[ H_3 \vdash e'_3 + H'_1 \]
\[ H_1 = H_3 + y \]
\[ H_1 \vdash e'_3 \rightarrow_r H_2 \mid E'[e'_2] \]
\[ E'' = y \ E' \]
\[ H_1 \vdash e'_3 \rightarrow_r H_2 \mid E'[e'_2] \]
\[ y \in H_2 \]
\[ \text{case } E = v \ E_1 \text{ where } v \text{ is not a variable.} \]
\[ [H_1]e'_1 = v \ E_1[e_1] \]
\[ e'_1 = v' \ e'_3 \]
\[ [H_1]v' = v \]
\[ [H_1]e'_3 = E_1[e_1] \]
\[ H_1 \vdash v' \ e'_3 + H'_1 \]
\[ H_1 \vdash v' \ l H_3 \]
\[ H_3 \vdash e'_3 + H'_1 \]
\[ H_1 = H_3 + f v(v') \]
\[ H_1 \vdash v' e'_3 \rightarrow H_1, z \mapsto v' \mid z e'_3 \]
\[ H_1, z \mapsto v' \ e'_3 + H'_1 + f v(v'), z \mapsto v' \]
\[ \text{I.H.} \]
\[ [H_2]E' = E_1 \]
\[ [H_2]e'_2 = e_1 \]
\[ E'' = z \ E' \]
\[ H_1 \vdash v' e'_3 \rightarrow_r H_2 \mid z E'[e'_2] \]
\[ f v(v') \in H_2 \]
\[ \text{case } E = v \ E_1 \ hearing e. \]
So

HEMSR-TR-2020-42, Nov 29, 2020,

\[ [H_1]e'_1 = \text{val } x = E_1[e_1]; e \]
\[ e'_1 = \text{val } x = e'_2; e'_3 \]
\[ [H_1]e'_2 = E_1[e_1] \]
\[ [H_1]e'_3 = e \]
\[ H_1 \vdash \text{val } x = E_1[e_1]; e \vdash H'_1 \]
\[ H_1 \vdash e'_2 \vdash H_3 \]
\[ H_1 \vdash e'_2 \rightarrow^* r H_2 \mid E'[e'_2] \]
\[ [H_2]E' = E_1 \]
\[ [H_2]e'_2 = e_1 \]
\[ E'' = \text{val } x = E'; e'_3 \]
\[ H_1 \vdash \text{val } x = e'_2; e'_3 \rightarrow^* r H_2 \mid \text{val } x = E'[e'_2]; e'_3 \text{ step} \]
\[ H_1 \vdash e'_1 \rightarrow^* r H_2 \mid E'[e'_2] \]
\[ H_2 \vdash \text{val } x = E'[e'_2]; e'_3 \vdash H'_1 \]
\[ \text{by substitution} \]
\[ \text{Lemma 15} \]
\[ \text{Lemma 2} \]
\[ \text{let} \]
\[ \text{fv}(e'_1) \in H_2, [x] \]
\[ [H_2]E'' = \text{val } x = [H_2]E'; [H_2]e'_3 \]
\[ = [H_2]E'[H_1]e'_3 \]
\[ = E_1 e \]
\[ \square \]

**Lemma 11. (Reference counting semantics is sound (big step, part 2))**

If \( E[e_1] \rightarrow E[e_2], \) and \( H_1 \text{ ok}, \) and \( E'[e'_1] \text{ ok}, \) and \( [H_1]E' = E, \) and \( [H_1]e'_1 = e_1, \) and \( H_1 \vdash E[e_1] \vdash H'_1, \) then there exists \( H_2, e'_2 \) such that \( H_1 \mid E'[e'_1] \rightarrow^* r H_2 \mid E'[e'_2], \) and \( [H_2]E' = E, \) and \( [H_2]e'_2 = e_2. \)

**Proof.** (Of Lemma 11) By induction on the evaluation context \( E. \) Note that following Lemma 15 and 2, we have \( \text{fv}(E') \in H_2. \)

**case** \( E = \square. \) Then \( E' = \square. \) The goal follows by Lemma 9.

**case** \( E = E_1 e, \) then \( E' = E'_1 e'. \)

\[ [H_1]E' = E_1 e \]
\[ [H_1]E'_1 = E' \]
\[ [H_1]e' = e \]
\[ E_1[e_1] \rightarrow E_1[e_2] \]
\[ H_1 \vdash E_1[e'_1] e' \vdash H'_1 \]
\[ H_1 \vdash E_1[e'_1] \vdash H_2 \]
\[ H_2 \vdash e' \vdash H'_1 \]
\[ H_1 \mid E_1[e'_1] \rightarrow^* r H_2 \mid E_1[e'_2] \]
\[ \text{I.H.} \]
\[ [H_3] e'_2 = e_2 \]
\[ H_1 \mid E_1[e'_1] e' \rightarrow^* r H_3 \mid E_1[e'_2] e' \]

**case** \( E = v E_1, \) then \( E' = x E'_1. \)

\[ [H_1]E' = v E_1 \]
\[ [H_1]x' = v \]
\[ E_1[e_1] \rightarrow E_1[e_2] \]
\[ H_1 \vdash x' E_1[e'_1] \vdash H'_1 \]
\[ H_1 \vdash x \vdash H_2 \]
\[ H_2 \vdash x E_1[e'_1] \vdash H'_1 \]
\[ H_1 = H_2 \# x \]
\[ H_1 \vdash E_1[e'_1] \vdash H'_1 \# x \]
\[ H_1 \mid E_1[e'_1] \rightarrow^* r H_3 \mid x E_1[e'_2] \]
\[ \text{I.H.} \]
\[ [H_3] e'_2 = e_2 \]
\[ H_1 \mid x E_1[e'_1] \rightarrow^* r H_3 \mid x E_1[e'_2] \]

**case** \( E = \text{val } x = E_1; e, \) then \( E' = \text{val } x = E'_1; e'. \)
\[ [H_1]E' = \text{val } x = E_1; e \]
\[ [H_1]E'_1 = E' \]
\[ [H_1]e' = e \]
\[ E_1[e_1] \rightsquigarrow E_1[e_2] \]
\[ H_1 \vdash \text{val } x = E'_1[e'_1]; e' + H'_1 \]
\[ H_1 \vdash E'_1[e'_1] + H_2 \]
\[ H_1 \mid E'_1[e'_1] \rightsquigarrow^r H_3 \mid E'_1[e'_2] \]
\[ \text{IH.} \]
\[ [H_3] e'_2 = e_2 \]
\[ H_1 \vdash \text{val } x = E'_1[e'_1]; e' \rightsquigarrow_r H_3 \mid \text{val } x = E'_1[e'_2]; e' \]
\[ \Box \]

**Lemma 12.** (*Reference counting semantics is sound (big step)*)

If \( e_1 \rightsquigarrow e_2 \) and \( H_1 \text{ ok} \), and \( e'_1 \text{ ok} \), and \( [H_1] e'_1 = e_1 \), and \( H_1 \vdash e'_1 + H'_1 \), then there exists \( H_2 \) and \( e'_2 \) such that \( H_1 \mid e'_1 \rightsquigarrow^r H_2 \mid e'_2 \), and \( [H_2] e'_2 = e_2 \).

**Proof.** (*Of Lemma 12*)

\( e_1 \rightsquigarrow e_2 \)
\( e_1 = E[e_1] \)
\( e_2 = E[e_2] \)
\( E[e_3] \rightsquigarrow E[e_4] \)
\( e'_1 = E_1[e'_1] \)
\( H_1 \mid E_1[e'_2] \rightsquigarrow^r H_2 \mid E_2[e'_3] \)
\( [H_2]E_2 = E \)
\( [H_2]e'_3 = e_3 \)
\( H_2 \text{ ok} \)
\( E_2[e'_4] \text{ ok} \)
\( H_2 \vdash E_2[e'_3] + H'_1 \)
\( H_3 \mid E_2[e'_3] \rightsquigarrow H_3 \mid E_2[e'_4] \)
\( [H_3]E_2 = E \)
\( [H_3]e'_4 = e_4 \)
\( [H_3](E_2[e'_4]) = ([H_3]E_2)\mid [H_3]e'_4 \) by substitution
\( = E[e_4] = e_2 \)
\( \Box \)

**Proof.** (*Of Theorem 1*)

\( \emptyset \vdash e \rightsquigarrow e' \) given
\( e \rightsquigarrow^* v \) given
\( e' \rightsquigarrow^* v' \) *Theorem 5*
\( H \text{ ok} \)
\( e' \text{ ok} \) from *LAM*
\( \emptyset \vdash e' \rightsquigarrow \emptyset \) *Lemma 7*
\( e' \rightsquigarrow^* r H_2 \mid v' \) *Lemma 12*
\( [H_2]v' = v \) above

**case** \( v' = x \). Then the goal is proved.

**case** \( v' \) is not a variable. Then by (*lam*) or (*con*) we have \( H_2 \mid v' \rightsquigarrow^* r H_2, z \rightsquigarrow^1 v' \mid z \), with \( z \) fresh. Then \( [H_2, z \rightsquigarrow^1 v'] z = [H_2, z \rightsquigarrow^1 v']v' = [H_2]v' = v. \)

\[ \Box \]

D.3 No Garbage

**D.3.1 Extending strict evaluation semantics.** If we add *dup* \( e \) and *drop* \( e \) in the syntax, as well as add to the standard semantics in Figure 6 the following rules:

\( (\text{dup}) \quad \text{dup } e' ; e \rightsquigarrow e \)
\( (\text{drop}) \quad \text{drop } e' ; e \rightsquigarrow e \)
we immediately see that translations does not change evaluation:

**Theorem 5. (Translation is sound)**
If \( e \mapsto^* v \) with \( \emptyset \vdash e \mapsto e' \), then also \( e' \mapsto^* v \).

**Proof. (Of Theorem 5)** Follows directly from Lemma 13 and the two reduction rule \((\text{dup})\) and \((\text{drop})\). \(\square\)

**Lemma 13. (Translation only inserts \text{dup/drop})**
If \( \Delta \vdash e \mapsto e' \) then \( e = [e'] \).

**Proof. (Of Lemma 13)** By straightforward case analysis of each derivation. \(\square\)

### D.3.2 Evaluation retains Heap Reference Counting.

**Definition 4. (Well-formed Abstractions)**
If \( e \vdash \), then all \( (\lambda^{ys} x. e) \) in \( e \) satisfies \( \llbracket ys, x \rrbracket \vdash e_1 \vdash \emptyset \).

**Definition 5. (Well-formed Heap)**
If \( H \vdash \), then (1) if \( x \mapsto^n v \in H \), then \( fv(v) \in H \), and \( v \vdash \); (2) there is no dependency cycles in \( H \).

**Lemma 14. (No Garbage (Small step))**
Given \( H_1 \vdash \) and \( e_1 \vdash \) if \( H_1 \vdash e_1 \vdash H' \), and \( H_1 \vdash e_1 \rightarrow_r H_2 \vdash e_2 \), then \( H_2 \vdash e_2 \vdash H' \).

**Proof. (Of Lemma 14)** When we a new variable \( z \mapsto^1 v \) in the heap (e.g., \((\text{lam})\)), \( z \) is fresh so its domain cannot refer to \( z \) (even indirectly). So there is no dependency cycle. Also, in those cases, since \( H_1 \vdash v \vdash H' \), by Lemma 2, we know \( fv(v) \in H_1 \). Moreover we have \( v \vdash \) as a precondition.

Heap reduction retains abstractions, with the only change being substitution. If \( \llbracket ys, x \rrbracket \vdash e \vdash \emptyset \), then \( \llbracket ys[y:=z], x \rrbracket \vdash e[y:=z] \vdash \emptyset \) by substitution.

Now we prove \( H_2 \vdash e_2 \vdash H' \) by induction on the judgment.

**case (app) \( H \mid \llbracket f \rrbracket z \rightarrow^r H \mid \llbracket \text{dup} \rrbracket ys \); \llbracket \text{drop} \rrbracket f \); \llbracket e[x:=z] \rrbracket \vdash (f \mapsto^n \lambda^{ys} x. e) \in H \)**

\[
H \vdash f \vdash H_1 \quad \text{given}
\]
\[
H_1 \vdash f \vdash z \quad H_2 \quad \text{Lemma 3}
\]
\[
y \in H_1 \vdash f \vdash z \quad f \mapsto \lambda^{ys} x. e \quad \text{by definition}
\]
\[
H \vdash \text{dup} \; ys \quad ; \quad \gamma \quad + \quad + \quad H_2 \quad \text{Lemma 4}
\]
\[
H \vdash ys \quad + \quad z \quad + \quad f \quad \quad \gamma \quad \quad \quad \lambda^{ys} x. e \quad \text{ok}
\]
\[
\llbracket ys, x \rrbracket \vdash e \vdash \emptyset \quad \lambda^{ys} x. e \quad \text{ok}
\]
\[
\llbracket ys, z \rrbracket \vdash e[x:=z] \vdash \emptyset \quad \text{by substitution}
\]
\[
H_1 \vdash ys \quad + \quad z \quad + \quad e[x:=z] \quad + \quad H_1 \quad \text{Lemma 8}
\]

**case (match) \( H \mid \llbracket \text{match} \rrbracket x \{ p_i \mapsto e_i \} \rightarrow^r H \mid \llbracket \text{dup} \rrbracket ys \); \llbracket \text{drop} \rrbracket x \); \llbracket e_i[xs:=ys] \rrbracket \text{ with } p_i = C \; xs \text{ and } (x \mapsto^n C \; ys) \in H \)**

\[
H \vdash \text{match} \; x \{ C \; xs \rightarrow e_i \} \rightarrow^r H' \quad \text{given}
\]
\[
H \vdash x \vdash H_1 \quad \text{given}
\]
\[
H_1, \llbracket xs \rrbracket \vdash e_i \vdash H' \quad \text{given}
\]
\[
xs \notin H_i \quad \text{given}
\]
\[
H \vdash H_1 \vdash x \quad \text{Lemma 3}
\]
\[
(x \mapsto^n C \; ys) \in H \quad \text{given}
\]
\[
y \in H \quad H \vdash \text{ok}
\]
\[
H \vdash \text{dup} \; ys \quad ; \quad \gamma \quad + \quad + \quad H_2 \quad \text{by definition}
\]
\[
H \vdash ys \quad + \quad x \quad + \quad ys \quad \gamma \quad \quad \quad \quad \lambda^{ys} x. e \quad \text{ok}
\]
\[
H_1 \vdash ys \quad + \quad x \quad + \quad H' \quad \text{Lemma 4}
\]
\[
H_1 \vdash e_i[ys:=ys] \quad + \quad H' \quad \text{by substitution}
\]

**case (lam) \( H \mid (\lambda^{ys} x. e) \rightarrow^r H, f \mapsto^1 \lambda^{ys} x. e \mid f \quad \text{fresh } f \)**
The ok part reasoning of Lemma 14 can be easily generalized to big step. So from now on we will implicitly assume every expression and heap we discuss is ok.

**Lemma 15. (No Garbage (big step))**

If $H_1 \vdash E[e_1] \rightarrow H'$, and $H_1 \vdash E[e_1] \rightarrow H_2 \vdash E[e_2]$, then $H_2 \vdash E[e_2] \rightarrow H'$.

**Proof. (Proof for Lemma 15)** By induction on $E$.

case $E = \square$. Follows by Lemma 14.

case $E = E_1 \ e$.

- $H_1 \vdash E_1[e_1] \ e \rightarrow H_2$ given
- $H_1 \vdash E_1[e_1] \rightarrow H_3$ DRAPP
- $H_3 \vdash e \rightarrow H_2$ given
- $H_1 \vdash E_1[e_2] \rightarrow H_3$ IH.
- $H_1 \vdash E_1[e_2] \ e \rightarrow H_2$ DRAPP

case $E = x \ E_1$.

- $H_1 \vdash x \ E_1[e_1] \rightarrow H_2$ given
- $H_1 \vdash x \rightarrow H_3$ DRAPP
- $H_3 \vdash E_1[e_1] \rightarrow H_2$ given
- $H_3 \vdash E_1[e_2] \rightarrow H_2$ IH.
- $H_1 \vdash x \ E_1[e_2] \rightarrow H_2$ DRAPP

case $E = \text{val} \ x = E_1; \ e$.

- $H_1 \vdash \text{val} \ x = E_1[e_1]; \ e \rightarrow H_2$ given
- $H_1 \vdash E_1[e_1] \rightarrow H_3$ DRBIND
- $H_3, x \rightarrow^1 () \vdash e \rightarrow H_2$ given
- $x \notin H_2$ given
- $H_1 \vdash E_1[e_2] \rightarrow H_3$ IH.
- $H_1 \vdash \text{val} \ x = E_1[e_2]; \ e \rightarrow H_2$ DRBIND

case $E = C \ x_1 \ldots x_n \ E_1 \ v_j \ldots v_n$. 
Theorem 6. (No garbage)
Given $\emptyset; \emptyset \vdash e \rightsquigarrow e_1$, and $\emptyset \vdash e_1 \mapsto^{\ldots} r H_i \vdash e_i$, then $H_i \vdash e_i \dashv \emptyset$.

Proof. (Of Theorem 6)

$\emptyset$ ok by construction
$e_1$ ok by lam
$\emptyset \vdash e_1 \dashv \emptyset$ Lemma 7
$H_i \vdash e_i \dashv \emptyset$ Lemma 15

D.3.3 No Garbage.

Lemma 16. (Reachability)
If $H_1 \vdash e \vdash H_2$, then there for all $y \in \text{dom}(H_1) - \text{dom}(H_2)$, reach$(y, H_1 | e)$. For ease of reference, we denote it as reach$(H_1 - H_2, H_1 | e)$

Proof. (Of Lemma 16) By induction on the judgment.

case

$H_0 \vdash C v_1 \ldots v_n \vdash H_n$ given
$H_0 \vdash v_1 \vdash H_1 \ldots H_{n-1} \vdash v_n \vdash H_n$ DRCON
reach$(H_{i-1} - H_i, H_{i-1} | v_i)$ I.H.
reach$(H_{i-1} - H_i, H_0 | v_i)$ Lemma 2
reach$(H_n - H_0, H_0 | C v_1 \ldots v_n)$ Follows

case

$H, x \mapsto^{n+1} v \vdash x \vdash H, x \mapsto^n v$ given
$\text{dom}(H, x \mapsto^{n+1} v) - \text{dom}(H, x \mapsto^n v) = \emptyset$

case

$H, x \mapsto^1 \lambda ys. e \vdash x \vdash H_1$ given
$H \vdash ys \mapsto H_1$ DRVARLAM
reach$(H - H_1, H | ys)$ I.H.
reach$(H - H_1, H | \lambda ys. e)$ by definition
reach$((H, x \mapsto^1 \lambda ys. e) - H_1, (H, x \mapsto^1 \lambda ys. e) | x)$ follows

case

$H, x \mapsto^1 C ys \vdash x \vdash H_1$ given
$H \vdash ys \mapsto H_1$ DRVARCON
reach$(H - H_1, H | ys)$ I.H.
reach$(H - H_1, H | C ys)$ by definition
reach$((H, x \mapsto^1 C ys) - H_1, (H, x \mapsto^1 C ys) | x)$ follows
H, x \mapsto^n v \vdash \text{dup } x; e \vdash H_1 \quad \text{given}
H, x \mapsto^{n+1} v \vdash e \vdash H_1 \quad \text{drdup}
reach((H, x \mapsto^{n+1} v) - H_1, (H, x \mapsto^{n+1} v) \mid e) \quad \text{I.H.}
reach((H, x \mapsto^n v) - H_1, (H, x \mapsto^n v) \mid \text{dup } x; e) \quad \text{follows}
\text{case}

H, x \mapsto^{n+1} v \vdash \text{drop } x; e \vdash H_1 \quad \text{given}
H, x \mapsto^n v \vdash e \vdash H_1 \quad \text{drdrop}
reach((H, x \mapsto^{n+1} v) - H_1, (H, x \mapsto^{n+1} v) \mid e) \quad \text{I.H.}
reach((H, x \mapsto^n v) - H_1, (H, x \mapsto^n v) \mid \text{drop } x; e) \quad \text{follows}
\text{case}

H, x \mapsto^1 C \, y : s \vdash \text{drop } x; e \vdash H_1 \quad \text{given}
H \vdash \text{drop } y : s; e \vdash H_1 \quad \text{drdropcon}
reach((H - H_1, H \mid \text{drop } y : s; e)) \quad \text{I.H.}
reach((H, x \mapsto^1 C \, y : s) - H_1, (H, x \mapsto^1 C \, y : s) \mid \text{drop } x; e) \quad \text{follows}
\text{case}

H, x \mapsto^1 \lambda y : s. z. e \vdash \text{drop } x; e \vdash H_1 \quad \text{given}
H \vdash \text{drop } y : s; e \vdash H_1 \quad \text{drdroplam}
reach((H - H_1, H \mid \text{drop } y : s; e)) \quad \text{I.H.}
reach((H, x \mapsto^1 \lambda y : s. z. e) - H_1, (H, x \mapsto^1 \lambda y : s. z. e) \mid \text{drop } x; e) \quad \text{follows}
\text{case}

H \vdash \lambda y : s. x. e \vdash H_1 \quad \text{given}
H \vdash y : s \vdash H_1 \quad \text{drlam}
reach((H - H_1, H \mid y : s)) \quad \text{I.H.}
reach((H - H_1, H \mid y : s. x. e)) \quad \text{follows}
\text{case}

H \vdash e_1 e_2 \vdash H_2 \quad \text{given}
H \vdash e_1 \vdash H_1 \quad \text{drapp}
H_1 \vdash e_2 \vdash H_2 \quad \text{drapp}
reach((H - H_1, H \mid e_1)) \quad \text{I.H.}
reach((H_1 - H_2, H_1 \mid e_2)) \quad \text{I.H.}
reach((H_1 - H_2, H \mid e_2)) \quad \text{Lemma 2}
reach((H - H_2, H \mid e_1 e_2)) \quad \text{follows}
\text{case}

H \vdash \text{val } x = e_1 ; e_2 \vdash H_2 \quad \text{given}
H \vdash e_1 \vdash H_1 \quad \text{drbind}
H_1, x \mapsto^1 () \vdash e_2 \vdash H_2 \quad \text{drbind}
x \notin H, H_1 \quad \text{drbind}
x \notin H, H_2 \quad \text{drbind}
x \notin H_1 - H_2, (H, x \mapsto^1 ()) \quad \text{I.H.}
x \notin H_1 - H_2, (H, x \mapsto^1 ()) \mid e_2 \quad \text{Lemma 2}
\text{dom}(H_1) \subseteq \text{dom}(H_1, x \mapsto^1 ())
reach((H_1 - H_2, (H, x \mapsto^1 ()) \mid e_2)) \quad \text{follows}
x \notin H \quad \text{dom}(H) - \text{dom}(H_2) \quad \text{known}
x \notin \text{dom}(H) \quad \text{dom}(H) - \text{dom}(H_2) \quad \text{known}
reach((H - H_2, H \mid \text{val } x = e_1 ; e_2)) \quad \text{follows}
\text{case}
D.4 Soundness of Syntax-directed Translation

Proof. (Of Theorem 2) By induction on the judgment.

case

\[ \Delta \mid x \mapsto x \quad \text{given} \]
\[ \Delta \mid x \vdash x \quad \text{VAR} \]

\[ \text{case} \]

\[ \Delta, \Delta_1 \mid \Gamma \mapsto_\Lambda \lambda x. e \leadsto \text{dup } \Delta_1; \lambda^{ys} x, e' \quad \text{given} \]
\[ x \in \text{fv}(e) \quad \text{SLAM} \]
\[ \emptyset \mid ys, x \mapsto_\Lambda e \leadsto e' \quad \text{SLAM} \]
\[ ys = \text{fv}(\lambda x. e) \quad \text{SLAM} \]
\[ \Delta_1 = ys - \Gamma \quad \text{SLAM} \]
\[ \emptyset \mid ys, x \vdash e \leadsto e' \quad \text{I.H.} \]
\[ \Delta, \Delta_1 \mid \Gamma \mapsto_\Lambda \lambda x. e \leadsto \lambda^{ys} x, e' \quad \text{LAM} \]
\[ \Delta, \Delta_1 \mid \Gamma \mapsto_\Lambda \lambda x. e \leadsto \text{dup } \Delta_1; \lambda^{ys} x, e' \quad \text{DUP} \]

\[ \text{case} \]

\[ \Delta, \Delta_1 \mid \Gamma \mapsto_\Lambda \lambda x. e \leadsto \text{dup } \Delta_1; \lambda^{ys} x, (\text{drop } x; e') \quad \text{given} \]
\[ x \notin \text{fv}(e) \quad \text{SLAM-DROP} \]
\[ \emptyset \mid ys \mapsto_\Lambda e \leadsto e' \quad \text{SLAM-DROP} \]
\[ ys = \text{fv}(\lambda x. e) \quad \text{SLAM-DROP} \]
\[ \Delta_1 = ys - \Gamma \quad \text{SLAM-DROP} \]
\[ \emptyset \mid ys \vdash e \leadsto e' \quad \text{I.H.} \]
\[ \emptyset \mid ys, x \mapsto e \leadsto \text{drop } x; e' \quad \text{DROP} \]
\[ ys = \text{fv}(\lambda x. \text{drop } x; e) \quad \text{follows} \]
\[ \Delta, \Delta_1 \mid \Gamma \mapsto_\Lambda \lambda x. e \leadsto \lambda^{ys} x, \text{drop } x; e' \quad \text{LAM} \]
\[ \Delta, \Delta_1 \mid \Gamma \mapsto_\Lambda \lambda x. e \leadsto \text{dup } \Delta_1; \lambda^{ys} x, e' \quad \text{DUP} \]
D.5 Precision

D.5.1 A Heap Reference Counting Calculus for the Algorithm.
\[
\frac{H \vdash s \ \cdot \ H_1 \ldots H_{n-1} \vdash s \ \cdot \ H_n}{H \vdash s \ C \ \cdot \ H_1 \ldots H_n} \quad \text{[SRCON]}
\]

\[
\frac{H, x \mapsto^{n+1} v \vdash s \ \cdot \ H, x \mapsto^{n} v}{H \vdash s \ \cdot \ H_1} \quad \text{[SRVAR]}
\]

\[
\frac{H, x \mapsto^{1} \ \lambda y x. \ e \vdash s \ \cdot \ H_1}{H \vdash s \ ys \ \cdot \ H_1} \quad \text{[SRVARLAM]}
\]

\[
\frac{H \vdash s \ ys \ \cdot \ H_1}{H, x \mapsto^{1} C \ ys \vdash s \ \cdot \ H_1} \quad \text{[SRVARCON]}
\]

\[
\frac{H \vdash s \ ys \ \cdot \ H_1 \ \cdot \ ys \mapsto^{1} () \mapsto^{1} () \vdash s \ e \ + \ \emptyset}{H \vdash s \ \lambda^{ys} x. \ e \ \cdot \ H_1} \quad \text{[SRLAM1]}
\]

\[
\frac{H \vdash s \ ys \ \cdot \ H_1 \ \cdot \ ys \mapsto^{1} () \vdash s \ e \ + \ \emptyset}{H \vdash s \ \lambda^{ys} x. \ drop \ e \ ; \ + \ H_1} \quad \text{[SRLAM2]}
\]

\[
\frac{H \vdash s \ e_1 \ + \ H_1 \ \cdot \ H_1 \vdash s \ e_2 \ + \ H_2}{H \vdash s \ e_1 \ e_2 \ + \ H_2} \quad \text{[SRAPP]}
\]

\[
\frac{H \vdash s \ e_1 \ + \ H_1 \ \cdot \ H_1 \vdash s \ e_2 \ + \ H_2 \ \cdot \ x \not\in H, H_2}{H \vdash s \ val \ x = e_1 \ ; \ e_2 \ + \ H_2} \quad \text{[SRBIND1]}
\]

\[
\frac{H \vdash s \ e_1 \ + \ H_1 \ \cdot \ H_1 \vdash s \ e_2 \ + \ H_2 \ \cdot \ x \not\in H}{H \vdash s \ val \ x = e_1 \ ; \ drop \ e_2 \ ; \ + \ H_2} \quad \text{[SRBIND2]}
\]

\[
\frac{H \vdash s \ x \ + \ H_1 \ \cdot \ H_1, [[\text{bv}(p_i)]] \vdash r \ \cdot \ drop \ ys_i; \ () \ + \ H_i}{H \vdash s \ e_i \ + \ H' \ \cdot \ \text{bv}(p_i) \not\in H, H'}
\]

\[
\frac{ys_i \subseteq \text{fv}(\{e_i\}) \cup \text{bv}(p_i)}{H \vdash s \ match \ x \ \cdot \ \{p_i \mapsto \text{drop } ys_i; \ e_i\} \ + \ H'} \quad \text{[SRMATCH]}
\]

\[
\frac{H, x \mapsto^{n+1} v \vdash s \ e \ + \ H_1}{H, x \mapsto^{n} v \vdash s \ \cdot \ dup \ x; \ + \ H_1} \quad \text{[SRDUP]}
\]

Where drop, and dup followed by drop are only allowed in:

\[
\frac{H, x \mapsto^{n+1} v \vdash r \ e \ + \ H_1}{H, x \mapsto^{n} v \vdash r \ dup \ x; \ + \ H_1} \quad \text{[RRDUP]}
\]

\[
\frac{H, x \mapsto^{n} v \vdash r \ e \ + \ H_1}{H, x \mapsto^{n+1} v \vdash r \ drop \ x; \ + \ H_1} \quad \text{[RRDROP]}
\]

\[
\frac{H \vdash r \ e \ + \ H_1}{H, x \mapsto^{1} () \vdash r \ drop \ x; \ + \ H_1} \quad \text{[RRDROPUNIT]}
\]

\[
\frac{H \vdash r \ \cdot \ drop \ ys; \ + \ H_1}{H, x \mapsto^{1} \ \lambda^{ys} x. \ e \vdash r \ drop \ x; \ + \ H_1} \quad \text{[RRDROPLAM]}
\]

\[
\frac{H \vdash r \ \cdot \ drop \ ys; \ + \ H_1}{H, x \mapsto^{1} C \ ys \vdash r \ drop \ x; \ + \ H_1} \quad \text{[RRDROPCONS]}
\]
H ⊢ s e + H_1 \quad [\text{RRSUB}]

D.5.2 Properties. Those properties are essentially the same as the lemma for the heap reference counting calculus.

Definition 6. (Well-formed Abstractions)
If $e \in ok_r$, then all $(\lambda y^s \ x. e_1)$ in $e$ satisfies (1) $[ys, x] \vdash r e_1 + \emptyset$; or (2) $e_1 = \text{drop } x$; $e_2$, and $[ys] \vdash r e_2 + \emptyset$.

Definition 7. (Well-formed Heap)
If $H ok$, then (1) if $x \mapsto^n v \in H$, then $fv(v) \in H$, and $v \in ok_r$; (2) there is no dependency cycles in $H$.

Lemma 17. (Heap Reference Counting Free variables)
If $H_1 \vdash r e + H_2$ or $H_1 \vdash s e + H_2$, then $fv(e) \in H_1$, and $fv(H_2) \in H_1$ with same domains.

Lemma 18. (Drop is dual to extension)
If $H_1 \vdash r \text{drop } x$; (1) $\vdash H_2$, then $H_1 = H_2 + x$. Similarly, if $H_1 \vdash r x + H_2$ or $H_1 \vdash s x + H_2$, then $H_1 = H_2 + x$.

Lemma 19. (Extension is dual to drop)
$H + x \vdash r \text{drop } x$; (1) $\vdash H$. Similarly, $H + x \vdash s x + H$ and $H + x \vdash s x + H$.

Lemma 20.
$[\Gamma, x] \vdash r x + [\Gamma]$. Similarly, if $[\Delta] \vdash r e \vdash H$, then $[\Gamma, x] \vdash r \text{drop } x$; $e \vdash H$.

Theorem 7. (No garbage)
Given $\emptyset; \emptyset \vdash r e \mapsto e_1$, and $\emptyset \vdash e_1 \mapsto^* r H_1 \mid e_1$, then $H_1 \vdash r e_1 \vdash \emptyset$.

D.5.3 Relating to linear resource calculus.

Lemma 21. (Algorithmic linear resource calculus relates to reference counting)
If $\Delta \mid \Gamma \vdash s e \mapsto e'$, then $[\Delta, \Gamma] \vdash s e' + [\Delta]$. By $\text{RRSUB}$ we also have $[\Delta, \Gamma] \vdash r e' + [\Delta]$.

Proof. (Of Lemma 21) During the proof, we reply on the fact that source program (i.e., $e$) has no drop or dup. By induction on the elaboration.

\begin{align*}
\text{case} & \\
\quad & \Delta \mid x \vdash s x \mapsto x \quad \text{given} \\
\quad & [\Delta, x] \vdash s x + [\Delta] \quad \text{Lemma 20} \\
\text{case} & \\
\quad \Delta, x \mid \emptyset \vdash s x \mapsto \text{dup } x; x \quad \text{given} & \\
\quad & [\Delta, x] \vdash x \vdash [\Delta, x] \quad \text{Lemma 19} \\
\quad & [\Delta, x] \vdash s \text{dup } x; x + [\Delta, x] \quad \text{SRDUP} \\
\text{case} & \\
\quad \Delta, \Delta_1 \mid \Gamma \vdash s \lambda x. e \mapsto \text{dup } \Delta_1; \lambda y^s x. e' \quad \text{given} & \\
\quad & x \in fv(e) \quad \text{SLAM} & \\
\quad & \emptyset \mid ys, x \vdash s e \mapsto e' \quad \text{SLAM} & \\
\quad & ys \equiv fv(\lambda x. e) \quad \text{SLAM} & \\
\quad & \Delta_1 = ys \mid \Gamma \quad \text{SLAM} & \\
\quad & [\Delta, \Delta_1, ys] \vdash s ys + [\Delta, \Delta_1] \quad \text{LH.} & \\
\quad & [\Delta, \Delta_1, \Gamma, \Delta_1] \vdash s ys + [\Delta, \Delta_1] \quad \text{Lemma 19} & \\
\quad & [\Delta, \Delta_1, \Gamma, \Delta_1] \vdash \lambda y^s x. e' + [\Delta, \Delta_1] \quad \text{by substitution} & \\
\quad & [\Delta, \Delta_1, \Gamma, \Delta_1] \vdash \lambda y^s x. e' + [\Delta, \Delta_1] \quad \text{SRSLAM} & \\
\text{case} & \\
\end{align*}
\[ \Delta, \Delta_1 \vdash \lambda x. e \rightsquigarrow \text{dup } \Delta_1; \lambda^{ys} x. \text{ (drop } x; e') \quad \text{ given} \]
\[ x \notin \text{fv}(e) \]  
\[ \emptyset \vdash ys \triangleright x \rightsquigarrow e' \]  
\[ ys \equiv \text{fv(}\lambda x. e) \]  
\[ \Delta_1 = ys \rightarrow \Gamma \]  
\[ ys \upharpoonright_t s \rightarrow e' \in \emptyset \]  
\[ [\Delta, \Delta_1, ys] \vdash_y s \rightarrow e' \in \Delta, \Delta_1 \]  
\[ \text{Lemma 19} \]  
\[ \text{SAML-DROP by substitution} \]  
\[ \text{SRLAM2} \]  
\[ \text{SRDUP} \]  
\[ \Delta \vdash \Gamma \vdash e_1 e_2 \rightsquigarrow e'_1 e'_2 \quad \text{given} \]  
\[ \Delta, \Gamma_2 \vdash \Gamma \rightarrow \Gamma_2 \vdash e_1 \rightsquigarrow e'_1 \quad \text{SAPP} \]  
\[ \Delta \vdash \Gamma \vdash e_1 e_2 \rightsquigarrow e'_1 e'_2 \quad \text{SAPP} \]  
\[ \Gamma_2 = \Gamma \cap \text{fv}(e_2) \quad \text{SAPP} \]  
\[ [\Delta, \Gamma] \vdash [\Delta, \Gamma_2] \quad \text{SRAPP} \]  
\[ \Delta \vdash \Gamma \vdash \text{val } x = e_1; e_2 \rightsquigarrow \text{val } x = e'_1; e'_2 \quad \text{given} \]  
\[ x \in \text{fv}(e_2) \]  
\[ \text{SBIND} \]  
\[ x \notin \Delta, \Gamma \]  
\[ \Delta, \Gamma_2 \vdash \Gamma \rightarrow \Gamma_2 \vdash e_1 \rightsquigarrow e'_1 \quad \text{SBIND} \]  
\[ \Delta \vdash \Gamma \vdash e_1 e_2 \rightsquigarrow e'_1 e'_2 \quad \text{SBIND} \]  
\[ \Gamma_2 = \Gamma \cap (\text{fv}(e_2) - x) \quad \text{SBIND} \]  
\[ [\Delta, \Gamma] \vdash [\Delta, \Gamma_2] \quad \text{L.H.} \]  
\[ [\Delta, \Gamma_2, x] \vdash [\Delta] \quad \text{L.H.} \]  
\[ x \notin [\Delta] \]  
\[ \text{follows} \]  
\[ [\Delta, \Gamma] \vdash [\Delta] \quad \text{SRBIND1} \]  
\[ \Delta \vdash \Gamma \vdash \text{val } x = e_1; e_2 \rightsquigarrow \text{val } x = e'_1; e'_2; \text{ drop } x; e'_2 \quad \text{given} \]  
\[ x \notin \text{fv}(e_2), \Delta, \Gamma \]  
\[ \Delta, \Gamma_2 \vdash \Gamma \rightarrow \Gamma_2 \vdash e_1 \rightsquigarrow e'_1 \quad \text{SBIND-DROP} \]  
\[ \Delta \vdash \Gamma \vdash e_1 e_2 \rightsquigarrow e'_1 e'_2 \quad \text{SBIND-DROP} \]  
\[ \Gamma_2 = \Gamma \cap \text{fv}(e_2) \quad \text{SBIND-DROP} \]  
\[ [\Delta, \Gamma] \vdash [\Delta, \Gamma_2] \quad \text{L.H.} \]  
\[ [\Delta, \Gamma_2] \vdash [\Delta] \quad \text{L.H.} \]  
\[ x \notin [\Delta, \Gamma] \]  
\[ [\Delta, \Gamma] \vdash [\Delta] \quad \text{follows} \]  
\[ \text{SRBIND2} \]  
\[ \Delta \vdash \Gamma \vdash \text{val } x = e'_1; \text{ drop } x; e'_2 \rightarrow [\Delta] \]  
\[ \text{case} \]
\[
\Delta \mid \Gamma, v_1 \ldots v_n \leadsto C v_1' \ldots v_n' \quad \text{given} \\
\Delta' \mid \Gamma, v_1 \ldots v_n \leadsto C v_1' \ldots v_n' \quad \text{smatch} \\
\Gamma_i \equiv (\Gamma, bv(p_i)) - \Gamma_i \\
\Delta' \mid \Gamma_i \vdash e_i' \quad \text{Lemma 20} \\
\Delta' \mid \Gamma_i \vdash C v_1 \ldots v_n \quad \text{Lemma 20} \\
\Delta' \mid \Gamma_i \vdash [\Delta, \Gamma_i] \quad \text{I.H.} \\
\Delta' \mid \Gamma_i \vdash e_i' \quad \text{assume \( bv(p_i) \) fresh} \\
\Delta' \mid \Gamma_i \vdash e_i' \quad \text{known} \\
\Delta' \mid \Gamma_i \vdash e_i' \quad \text{invariant} \\
\Delta' \mid \Gamma_i \vdash e_i' \quad \text{definition of \( fv \)} \\
\Delta' \mid \Gamma_i \vdash e_i' \quad \text{follows} \\
\Delta' \mid \Gamma_i \vdash e_i' \quad \text{by substitution} \\
\Delta' \mid \Gamma_i \vdash e_i' \quad \text{srmatch} \\
\\]

\section*{D.5.4 Precision.}

\textbf{Lemma 22.} \textit{(Reachability for erased expressions)}

If \( H_1 \vdash_s e \rightarrow H_2 \), then \( \text{reach}(H_1 - H_2, H_1 \mid [e]) \).

\textbf{Proof.} (Of Lemma 22) By induction on the judgment.

\textbf{case}

\[
H \vdash_s C v_1 \ldots v_n + H_1 \quad \text{given} \\
H \vdash_s v_1 + H_1 \ldots H_{n-1} + s v_n + H_n \quad \text{scon} \\
\Delta \mid \Gamma_i \vdash e_i' \quad \text{Lemma 17} \\
[H \vdash \Delta \mid \Gamma_i \vdash e_i'] \quad \text{L.H.} \\
[\Delta, \Gamma_i \vdash e_i'] \quad \text{follows} \\
\]
\( H, \; x \mapsto 1 \; C \; ys \vdash x - | H_1 \) given
\( H \vdash s \; ys \vdash H_1 \) srvarcon
reach\((H - H_1, \; H \{ \left[ ys \right]\})\) LH.
reach\((H - H_1, \; H \{ \left[ C \; ys \right]\})\) by definition
reach\((H, \; x \mapsto 1 \; C \; ys - H_1, \; (H, \; x \mapsto 1 \; C \; ys) \{ \left[ x \right]\})\) follows
\textbf{case}

\( H \vdash s \; \lambda^{ys} \; x \cdot e \vdash H_1 \) given
\( H \vdash s \; ys \vdash H_1 \) srlam1
reach\((H - H_1, \; H \{ \left[ ys \right]\})\) LH.
reach\((H - H_1, \; H \{ \left[ \lambda^{ys} \; x \cdot e \right]\})\) follows
\textbf{case}

\( H \vdash s \; e_1 \; e_2 \vdash H_2 \) given
\( H \vdash s \; e_1 \vdash H_1 \) srapp
\( H_1 \vdash s \; e_2 \vdash H_2 \) srapp
reach\((H - H_1, \; H \{ \left[ e_1 \right]\})\) LH.
reach\((H_1 - H_2, \; H_1 \{ \left[ e_2 \right]\})\) LH.
reach\((H_1 - H_2, \; H \{ \left[ e_2 \right]\})\) Lemma 17
reach\((H - H_2, \; H \{ \left[ e_1 \; e_2 \right]\})\) follows
\textbf{case}

\( H \vdash s \; \text{val} \; x = e_1 ; \; e_2 \vdash H_2 \) given
\( H_1, \; x \mapsto 1 \; (\) \vdash s \; e_2 \vdash H_2 \) srbind1
\( x \notin H, \; H_2 \) srbind1
reach\((H - H_1, \; H \{ \left[ e_1 \right]\})\) LH.
reach\(((H_1, \; x \mapsto 1 \; (\) - H_2, \; (H_1, \; x \mapsto 1 \; (\) \{ \left[ e_2 \right]\})\) LH.
reach\(((H_1, \; x \mapsto 1 \; (\) - H_2, \; (H, \; x \mapsto 1 \; (\) \{ \left[ e_2 \right]\})\) Lemma 17
dom\((H_1) \subseteq \text{dom}(H_1, \; x \mapsto 1 \; (\))
reach\((H_1 - H_2, \; (H, \; x \mapsto 1 \; (\) \{ \left[ e_2 \right]\})\) follows
\( x \notin H \) known
\( x \notin \text{dom}(H) - \text{dom}(H_2) \) follows
reach\((H - H_2, \; H \{ \text{val} \; x = e_1 ; \; e_2 \})\) follows
\textbf{case}

\( H \vdash s \; \text{val} \; x = e_1 ; \; \text{drop} \; x ; \; e_2 \vdash H_2 \) given
\( H \vdash s \; e_1 \vdash H_1 \) srbind2
\( H_1 \vdash s \; e_2 \vdash H_2 \) srbind2
\( x \notin H \) srbind2
reach\((H - H_1, \; H \{ \left[ e_1 \right]\})\) LH.
reach\(((H_1 - H_2, \; H_1 \{ \left[ e_2 \right]\})\) LH.
reach\(((H_1 - H_2, \; H \{ \left[ e_2 \right]\})\) Lemma 17
\( x \notin H \) known
\( x \notin \text{dom}(H) - \text{dom}(H_2) \) follows
reach\((H - H_2, \; H \{ \text{val} \; x = e_1 ; \; \text{drop} \; x ; \; e_2 \})\) follows
\textbf{case}
\[
H \vdash_s \text{match } x \{ p_i \mapsto \text{drop } y s_i ; e_i \} \rightarrow H' \quad \text{given}
\]
\[
H \vdash_s x \rightarrow H_1
\]
\[
H_1, [\text{bv}(p_i)] \vdash_r \text{drop } y s_i ; () \rightarrow H_i
\]
\[
H \vdash_s e_i \rightarrow H'
\]
\[
\text{bv}(p_i) \notin H, H'
\]
\[
y s_i \subseteq \text{fv}(\lceil e_i \rceil) \cup \text{bv}(p_i)
\]
\[
\text{reach}(H - H_1, H \mid x)
\]
\[
H_1, [\text{bv}(p_i)] = H_i + y s_i
\]
\[
\text{Lemma 18}
\]
\[
\text{reach}((H_i - H', H_i \mid \lceil e_i \rceil))
\]
\[
\text{Lemma 17}
\]
\[
y s_i \subseteq \text{fv}(\lceil e_i \rceil) \cup \text{bv}(p_i)
\]
\[
\text{reach}((H_i + y s_i - H', H \mid \text{bv}(p_i); \lceil e_i \rceil))
\]
\[
\text{follows}
\]
\[
\text{reach}((H_i, [\text{bv}(p_i)] - H', H \mid \text{bv}(p_i); \lceil e_i \rceil))
\]
\[
\text{by substitution}
\]
\[
\text{bv}(p_i) \notin H
\]
\[
\text{known}
\]
\[
\text{bv}(p_i) \notin \text{dom}(H) - \text{dom}(H')
\]
\[
\text{follows}
\]
\[
\text{reach}(H - H', H \mid \text{match } x \{ p_i \mapsto [e_i] \})
\]
\[
\text{follows}
\]

\textbf{case}

\[
H, x \mapsto^n v \vdash_s \text{dup } x; e \rightarrow H_1
\]
\[
\text{given}
\]
\[
H, x \mapsto^{n+1} v \vdash_s e \rightarrow H
\]
\[
\text{SDUP}
\]
\[
x \in \text{fv}([e_i])
\]
\[
\text{SDUP}
\]
\[
\text{reach}((H, x \mapsto^n v) - H, (H, x \mapsto^{n+1} v) \mid e)
\]
\[
\text{L.H.}
\]
\[
\text{reach}((H, x \mapsto^n v) - H, (H, x \mapsto^n v) \mid e)
\]
\[
\text{Follows}
\]

\[\Box\]

\textbf{Proof. (Of Theorem 4)}

\[
\emptyset \mid \emptyset \vdash_s e \rightarrow e'
\]
\[
\text{given}
\]
\[
\emptyset \vdash_r e' \rightarrow \emptyset
\]
\[
\text{Lemma 21}
\]
\[
H_i \vdash_r e_i \rightarrow \emptyset
\]
\[
\text{Theorem 7}
\]
\[
e_i \notin E[\text{dup } x; e'_i]
\]
\[
\text{given}
\]
\[
H_i \vdash_s e' \rightarrow \emptyset
\]
\[
\text{RRSUB}
\]
\[
\text{reach}(H_i - \emptyset, H_i \mid \lceil e \rceil)
\]
\[
\text{Lemma 22}
\]
\[
\text{all } y \in \text{dom}(H_i), \text{reach}(y, H_i \mid e_i)
\]
\[
\text{follows}
\]

\[\Box\]