Fungi: Typed incremental computation with names

MATTHEW A. HAMMER, University of Colorado Boulder
JANA DUNFIELD, Queen’s University
KYLE HEADLEY, University of Colorado Boulder
MONAL NARASIMHAMURTHY, University of Colorado Boulder
DIMITRIOS J. ECONOMOU, University of Colorado Boulder

Incremental computations attempt to exploit input similarities over time, reusing work that is unaffected by input changes. To maximize this reuse in a general-purpose programming setting, programmers need a mechanism to identify dynamic allocations (of data and subcomputations) that correspond over time.

We present Fungi, a typed functional language for incremental computation with names. Unlike prior general-purpose languages for incremental computing, Fungi’s notion of names is formal, general, and statically verifiable. Fungi’s type-and-effect system permits the programmer to encode (program-specific) local invariants about names, and to use these invariants to establish *global uniqueness* for their composed programs, the property of using names correctly. We prove that well-typed Fungi programs respect global uniqueness.

We derive a bidirectional version of the type and effect system, and we have implemented a prototype of Fungi in Rust. We apply Fungi to a library of incremental collections, showing that it is expressive in practice.

1 INTRODUCTION

In many software systems, a fixed algorithm runs repeatedly over a series of *incrementally changing* inputs (Inp₁, Inp₂, ...), producing a series of *incrementally changing* outputs (Out₁, Out₂, ...). For example, programmers often change only a single line of source code and recompile, so Inpᵣ is often similar to Inpᵣ₋₁.

The goal of incremental *computation* is to exploit input similarity by reusing work from previous runs. If the source code Inpᵣ is almost the same as Inpᵣ₋₁, much of the work done to compile Inpᵣ and produce the target Outᵣ can be reused. In many settings, this reuse leads to asymptotic improvements in running time.

Such improvements are possible when the recomputation is *stable*: when the work done by run t − 1, producing output Outᵣ₋₁ from input Inpᵣ₋₁, is similar to the work needed for run t to produce output Outᵣ from Inpᵣ. In some cases, such as total replacement of the source program being compiled, stability is impossible. Thus, a central design question is how to maximize stability.

Consider a simple program that applies a binary operation g to two parts (x, y) of the input, and then applies another binary operation f to the result of g and a third part (z) of the input. This program has three inputs, one output, and one *intermediate result* (the result of g on x and y).
Assuming efficient equality tests for $x$, $y$ and the result of $g$, we can save this intermediate result and, potentially, reuse it across runs.

Fig. 1 shows some example runs. In the first run, we have stored $g(x, y)$. In the second run, the user has changed the input $z$ to $z'$—but since the inputs $x$ and $y$ have not changed, we can reuse the result $g(x, y)$ and perform only the operation $f$. In the third run, the user has changed $x$ to $x'$, which requires doing the operation $g$ again.

Thus, between the first and second runs we had to recompute only $f$; between the second and third runs, we had to recompute $g$. Depending on whether $g$’s result changes, we might recompute $f$ as well.

At this low level of complexity, it may seem straightforward to ensure that the incremental program is both consistent and efficient:

- An incremental program is **from-scratch consistent** if its output matches the output that would be produced by running the program from scratch (that is, without using saved intermediate results).
- An incremental program is **incrementally efficient** (or achieves incremental efficiency) if it does only the necessary new work.

For nontrivial programs, however, achieving both incremental consistency and incremental efficiency can be extremely difficult. Consider GNU make, a relatively simple build system: it achieves consistency (at least in principle) only by working at a very coarse level of granularity—entire programs ($cc$, $ld$, etc.) and entire files. Opportunities to reuse work within a 5,000-line input to $cc$ are missed, and understandably so: compilers are large systems that use complex data structures and clever algorithms. Merely comparing file modification times (or even file contents) cannot utilize, say, the fact that the result of a liveness analysis has not changed. (Or, that the analysis has changed slightly, which creates many subtle dependencies.)

The gold standard for incremental programs is to painstakingly design an incremental algorithm that explicitly saves results and reuses work, perhaps in very clever ways. In many development settings, it is not feasible to expend that kind of effort. Rather than giving up on incremental software (by not attempting to reuse work at all) or using simplistic approaches (along the lines of make) that miss many opportunities for reuse, we should offer incremental programming languages that allow programmers to easily build incremental programs that are correct and efficient, at scale. Thus, an incremental programming language should enable programmers (1) to store and reuse intermediate results, without drastically changing their source program; (2) to exploit similarities (between inputs, and between stored results), including for highly structured input data and nontrivial data.
structures; (3) to easily combine smaller incremental programs into incremental systems. Moreover, the language should make it as easy as possible to obtain both correctness and efficiency.

Incremental languages can be categorized by their breadth of applicability, with domain-specific languages at one end of the spectrum and general-purpose languages at the other; the language in this paper is general-purpose. The central advance we make is in statically verifying an important aspect of incremental programs: that subcomputations are named uniquely within each run.

The tiny program shown above is not adequate to illustrate the need for unique naming: the program’s input has no interesting structure, and there is only one intermediate result. We argue the need for names themselves here; we will discuss a concrete example, illustrating the need for unique names, in Sec. 2.

To reuse a unit of work, we must observe that the newer result corresponds to the older result. The program $f(g(x, y), z)$ uses no control structures and performs the operations $f$ and $g$ exactly once, so it is immediate that $g(x, y)$ in the second run corresponds to $g(x, y)$ in the first run. Moreover, we say that $g(x', y)$ in the third run corresponds to $g(x, y)$ in the second run, even though $x'$ is (probably) not equal to $x$ and hence $g(x', y)$ is (probably) not equal to $g(x, y)$: Correspondence is not equality; instead, correspondence is the idea that two uses of $g$ happen “in the same place”.

The correspondence of $x'$ to $x$, and $z'$ to $z$, is even more immediate. But what if, instead of giving three discrete inputs ($x, y, z$), we gave a list of integers as input? If the change in input across runs is confined to specific list elements, say replacing the second element 22 with 23, we could say that the $k$th element of the previous input corresponds to the $k$th element of the current input. However, if the change is to insert an element in the input list, identifying the $k$th element at time $t - 1$ with the $k$th element at time $t$ won’t work: the small change of inserting a single element will look like the complete replacement. We need some notion of identity to realize that, if we insert an element at (say) the head of the list, the $1$st element at time $t - 1$ corresponds to the $2$nd element at time $t$, the $2$nd element at time $t - 1$ corresponds to the $3$rd element at time $t$, and so forth.

In our setting of a general-purpose language, there is no one-size-fits-all notion of identity. Instead, we need to enable programmers to choose a notion of identity that is appropriate for each program—a notion that exposes appropriate correspondences, and hence enables reuse. We call this notion of identity a naming strategy. Choosing a naming strategy that actually enables reuse is often difficult; the study of incremental cost semantics, which describe the potential for reuse, is a research area in itself. Our contribution is to make it easier for programmers to experiment with different naming strategies: the Fungi type system rules out a large class of naming errors that, in earlier languages such as Nominal Adapton [Hammer et al. 2015], could only be caught at run time.

In Table 1, we compare Fungi to some related approaches. The first two rows list work on incremental languages for substantially different programming models; those systems’ answers to the question of how to identify corresponding subcomputations do not apply in our setting (nor would our answer apply in theirs). We briefly discuss these two systems, and other work in substantially different settings, in Section 8. The remaining rows in the table—starting with AFL [Acar et al. 2002]—list general-purpose incremental programming languages that endeavor to provide a standard programming model with (relatively) lightweight incrementality; as we noted above, we want to support incrementality without requiring programmers to drastically change their source programs. Within this broad setting, we can observe an evolution from no mechanism to identify corresponding subcomputations (AFL in 2002) to informal or specialized mechanisms (several papers through 2012 and Adapton in 2014), and then to formal mechanisms.

Contributions. We make the following contributions:

- We develop a type-and-effect system for a general-purpose incremental programming language (Sections 3 and 4). Using refinement types, the system statically relates names to
Table 1. Some approaches to incremental computation

<table>
<thead>
<tr>
<th>approach</th>
<th>programming model</th>
<th>mechanism to identify corresponding subcomputations</th>
<th>detection of naming errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demetrescu et al. [2011]</td>
<td>reactive/imperative</td>
<td>memory address</td>
<td>n/a</td>
</tr>
<tr>
<td>Concurrent revisions</td>
<td>revision-based</td>
<td>call graphs (1)</td>
<td>n/a</td>
</tr>
<tr>
<td>[Burckhardt et al. 2011]</td>
<td>imperative programming</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AFL [Acar et al. 2002]</td>
<td>functional language</td>
<td>none</td>
<td>n/a</td>
</tr>
<tr>
<td>Carlsson [2002]</td>
<td>functional language</td>
<td>none</td>
<td>n/a</td>
</tr>
<tr>
<td>Acar et al. [2006b,a]</td>
<td>functional language</td>
<td>keys (informal)</td>
<td>(2)</td>
</tr>
<tr>
<td>DeltaML [Acar and Ley-Wild 2008]</td>
<td>functional language</td>
<td>keys (informal)</td>
<td>(2)</td>
</tr>
<tr>
<td>CEAL [Hammer et al. 2009]</td>
<td>imperative language</td>
<td>keys (informal)</td>
<td>(2)</td>
</tr>
<tr>
<td>implicit SAC [Chen et al. 2011, 2012]</td>
<td>functional language</td>
<td>keys (informal)</td>
<td>(2)</td>
</tr>
<tr>
<td>Adapton [Hammer et al. 2014]</td>
<td>functional language</td>
<td>structural (hash-consing)</td>
<td>n/a</td>
</tr>
<tr>
<td>Nominal Adapton [Hammer et al. 2015]</td>
<td>functional language</td>
<td>names (formal)</td>
<td>dynamic</td>
</tr>
<tr>
<td>Fungi (this paper)</td>
<td>functional language</td>
<td>names (formal)</td>
<td>static</td>
</tr>
</tbody>
</table>

(1) position in global call graph; small changes in call graph structure prevent reuse
(2) fall back to a global counter—preventing reuse now, in the future, or both

allocated data (references) and computations (thunks); it supports a set of type-level operations on names that is large enough to describe sophisticated uses of names, but small enough for decidable type checking.

- In Section 6, we prove that the effects tracked by our system are sound with respect to our dynamic semantics (Section 5). As a consequence, our type system ensures, statically, that names are unique within each run of the program—a property that, previously, could only be checked dynamically [Hammer et al. 2015]. In nontrivial programs, this global uniqueness property is a consequence of local uniqueness properties that are specific to particular algorithms and data structures; see Section 2.

- We implement the type system, and demonstrate its applicability to a variety of examples (Section 7).

2 OVERVIEW

In this section, we use an example program to give an overview of Fungi as a typed language for incremental computation with names. Specifically, we consider the from-scratch semantics, typing, and incremental semantics of dedup, a list-processing function that removes duplicates: the output list retains only the first occurrence of each input list element.

The implementation of dedup uses names to create correspondences between similar inputs, leading to incremental reuse via an efficient application of a (general-purpose) change propagation algorithm. The correctness of change propagation relies on the global uniqueness of allocation names, explained below.

The Fungi type system ensures that dedup satisfies global uniqueness; to do so, the Fungi programmer uses types to express several local uniqueness invariants. Before discussing this example, we briefly discuss these naming properties, which are each fundamental to the novel design of Fungi as a language for typed incremental computation with names.
2.1 Naming properties
Our Fungi type system enforces the global uniqueness of names. For nontrivial programs, global uniqueness requires local uniqueness of names; our type system also checks local uniqueness properties as stated by the programmer.

Global uniqueness of allocation names: For every allocated reference cell or thunk, the name used to identify the allocated reference (or thunk) is unique.

Local uniqueness properties: The data structures in an incremental program may contain names. For example, if we map over a list, we may need to associate the third element of the input list with the third element of the output list. The name used to represent “being the third element” may then occur within related pointer names, such as the pointer names of the third element of the input and the third element of the output. The name that represents “being the third element” may be stored in several different lists, but it should not occur more than once within each list: the input list cannot have two third elements. Since the appropriate local uniqueness properties depend on the details of each program, they cannot be given a priori. Instead, the programmer or library designer expresses the appropriate properties, using the Fungi type system.

In general, local uniqueness—in the form appropriate to each program—is needed to ensure global uniqueness. Our type system rules out, statically, violations of global uniqueness and violations of local uniqueness. While previous systems such as Nominal Adapton included constant-time dynamic checks to catch violations of global uniqueness, most local uniqueness properties cannot be checked in constant time.

Since local uniqueness violations can lead to subsequent global uniqueness violations, being able to statically ensure local uniqueness rules out a large class of subtle errors—much like the advanced type system of the Rust language rules out dangling pointers. As we show below (Sec. 2.6), some violations in these principles are only triggered by certain inputs, which may be unlikely, and thus unlikely to show up in randomized dynamic tests.

By enforcing these principles of unique names statically, Fungi programs enjoy the guarantees they afford, e.g., that change propagation will work correctly.

These principles about names, which are fundamental to general-purpose incremental computation, have been applied in some incremental computing systems of the past, but until now, have not been codified formally, or statically verified (see Table 1 for details).

In some past systems (based on self-adjusting computation), the runtime dynamically detects and tolerates violations of these uniqueness properties—the names are called "keys", and are viewed as hints that can be wrong, or non-unique. In the cases that they are not unique, the caching/allocation mechanism falls back to using a global counter. In turn, this cache location choice is not based on the current input, is not functional, and consequently, it will generally not be reusable as a "replayed" allocation in subsequent invocations of change propagation on similar inputs.

In other systems (Nominal Adapton), the runtime system simply triggers a dynamic error for violations of global uniqueness.

No prior system of which we are aware permits programmers to systematically encode or check local uniqueness, either statically, or dynamically (which would be expensive).

Next, to make these ideas concrete, we consider an example.

2.2 The program listing and dynamic semantics of dedup
Fig. 2 gives the program listing for dedup, including type declarations. The right-hand column of the figure shows additional type declarations, explained further below (Sec. 2.4).
First, let’s consider an approximation of the declared type and code for dedup, ignoring the index term declaration (\texttt{idxtm Dedup}) and other type indices and effects. The type declaration of \texttt{dedup} says that it accepts two arguments, a list of type \texttt{List[X1]} and a hash trie of type \texttt{Trie[X2]}, and returns a list of type \texttt{List[X1]}. Before examining the type structure of \texttt{dedup} in more detail, we consider the code, and its dynamic semantics.

Consider the initial run of \texttt{dedup} on the input list $[3, 4, 3, 9]$, stored at the sequence of pointer addresses $(a_1, a_2, a_3, a_4, a_5)$, which store \texttt{Cons} cells and a terminal \texttt{Nil} value. In addition to the elements $[3, 4, 3, 9]$, the \texttt{Cons} cells also contain a sequence of names (as values) $\langle n_1, n_2, n_3, n_4 \rangle$, with one name per \texttt{Cons} cell.

The \texttt{dedup} function uses these names to determine its allocation names—the identities of allocated data and thunks. Moreover, it stores these names (as values) within the allocated data. Intuitively, these names identify the logical places of the \texttt{Cons} cells in the input list, and by copying these names into these other allocated values, they permit the \texttt{dedup} program to create correspondences with other logical places in its data. Further below, we will look at a full picture of this entire execution.
We briefly describe the structure of names, and discuss a notion that underpins Fungi’s design: apartness of names, name sets and name functions.

Our core calculus defines names as binary trees, \( \text{name} ::= \text{leaf} | \langle \text{name}, \text{name} \rangle \). In practice, we augment this definition in two small ways. First, we extend the \text{leaf} production with other terminal productions for numbers and symbolic constants, written \text{0} and \text{t} (respectively) in the example above. For the purposes of reasoning formally, we assume (unspecified) encodings of these terminal productions into the simple formal grammar above. Second, we use a more lightweight notation for binary
name composition: \( n_1 \cdot n_2 \cdot n_3 \) denotes \( \langle \langle n_1, \langle n_2, n_3 \rangle \rangle \rangle \). This is only a convenient notation; names are still trees, so (unlike string concatenation) binary name composition is not associative: \( n_1 \cdot n_2 \cdot n_3 \neq (n_1 \cdot n_2) \cdot n_3 \), since \( \langle \langle n_1, \langle n_2, n_3 \rangle \rangle \rangle \neq \langle \langle \langle n_1, n_2 \rangle, n_3 \rangle \rangle \).

To respect the principles of unique names, Fungi encodes “uniqueness” through apartness. Apartness plays a central role in our type-and-effects system and metatheory. In Fungi code, we read the connective \( \perp \) as “apart”, a notion that (1) generalizes the operation of (disjoint) set union and (2) asserts that the left- and right-hand operands are indeed disjoint, with no common names.

Unlike disjoint set union, which is only defined for sets, our type system defines apartness over (pairs of) name terms and index terms. Name terms include functions over names, as well as literal names; index terms include name sets. Informally, we say that (1) two names \( n_1 \) and \( n_2 \) are apart if they are not equal (if \( n_1 \) and \( n_2 \) are distinct binary trees), (2) two sets of names are apart if they are disjoint, and (3) two functions are apart if the functions’ images are apart. For example, two functions from names to names are apart if their images (name sets) are apart.

### 2.4 Static effects and types for dedup

Having seen part of a dynamic execution, we consider a static view of dedup, how Fungi enforces global uniqueness for it, and how Fungi permits the programmer to express and enforce the local uniqueness invariants that support global uniqueness.

**Global uniqueness: Static effects for dedup.** Returning to Fig. 2, the index term declaration \textit{idxtm} \texttt{Dedup} defines a function from name sets to name sets, of sort \texttt{NmSet \rightarrow NmSet}. Given the names in dedup’s input list, the name set function \texttt{Dedup} gives an overapproximation of dedup’s write set—the set of names written by executing dedup on an input list associated with the given name set. This name set function \texttt{Dedup} appears in the type of \texttt{Dedup}, defining the write set in terms of \texttt{X1} as \( \triangleright \) \[\text{Dedup X1}\].\footnote{Our full type system also tracks read sets, and checks that the read and write sets are in harmony: it is not possible to read a location before it has been allocated.} This annotation says that \texttt{Dedup} is a static abstraction of the dynamic allocation effects in the body of dedup.

As explained in detail above, dedup uses each input name \( x \) (drawn from name set \( \text{X1} \)) three times. However, in each of these uses \( x \) is composed with other name constants, resulting in unique global names. The three uses are as follows.

1. **Allocate a new path in the trie.** In aggregate, these allocations write names in the set \texttt{Insert X1}, but with the name constant \( \text{@t} \) prepended.
2. **Allocate a recursive thunk.** In aggregate, these allocations write names in \( \text{X1} \), but with the name constant \( \text{@dd} \) prepended.
3. **Allocate an output list cell.** In aggregate, these allocations write some names in \( \text{X1} \) (for names of non-duplicated input list elements), but with the name constant \( \text{@r} \) prepended.

These three terms appear in the body of \texttt{Dedup}. To describe pointwise binary name combination over pairs of name sets, Fungi uses the notation \texttt{•}. (Above, we write “·” and “•” for binary combination of name constants and name values, respectively.) Using the apart name set operator \( \perp \), the body of \texttt{Dedup} combines these three (disjoint) subsets, simultaneously asserting that they stand apart.
To see why these terms indeed stand apart, consider the following expansion, where we expand the definition of Dedup over \{n_2\}, to account for the write set of the \(n_2\) tile only (Fig. 3):

\[
\text{Dedup}\{n_2\} = \begin{cases}
\{t\} \cdot \text{Insert}\{n_2\} & \downarrow \{dd\} \cdot \{n_2\} \downarrow \{r\} \cdot \{n_2\} \\
\{t\} \cdot \{n_2\} \cdot \text{Nat} & \downarrow \{dd\} \cdot \{n_2\} \downarrow \{r\} \cdot \{n_2\}
\end{cases}
\]

\[
= \{t\} \cdot \{n_2\} \cdot \text{Succ}^*\{\text{Zero}\} & \downarrow \{dd\} \cdot \{n_2, r\} \\
= \{t\} \cdot \{n_2\} \cdot \text{Succ}^*\{\text{Succ}\{\text{Zero}\}\} & \downarrow \{dd\} \cdot \{n_2, r\}
\]

\[
= \{t\} \cdot \{n_2\} \cdot \text{Succ}^*\{\text{Succ}\{\text{Zero}\}\} & \downarrow \{t \cdot \{n_2^2\} \cdot \text{Zero}, \{dd\} \cdot \{n_2, r\}\}
\]

\[
= \{t\} \cdot \{n_2\} \cdot \text{Succ}^*\{\text{Succ}\{\text{Zero}\}\} & \downarrow \{t \cdot \{n_2^2\} \cdot \text{Zero}, \{dd\} \cdot \{n_2, r\}\}
\]

The definition of Insert uses Nat, an infinite set defined by Kleene closure: Succ^*\{Zero\}. Sec. 2.5 explains this definition and the corresponding implementation of insert, but note that the “unrolled” set includes the five names that appear in Fig. 3 that are each based on \(n_2\), with \(t\) prepended and \(0\–4\) appended. We use decimal notation in place of the actual unary Zero and Succ.

As this expansion shows, the names in the image of Dedup \{n_2\} are pairwise distinct: we can distinguish them by their prefixes (\(t\), \(dd\) and \(r\)), or—for those with the common prefix \(t\)—by their distinct suffix \(0\–4\).

What about the other tiles, for input positions \(n_1\), \(n_3\) and \(n_4\)? Global uniqueness for the entire execution of dedup rests on the assumptions of local uniqueness for the input list and input trie, e.g., that \(n_2\) is distinct from all other names, which are also pairwise distinct. Next, we explain how the Fungi programmer establishes and maintains the local uniqueness invariants.

**Local uniqueness:** Type indices for dedup. The Fungi programmer encodes local uniqueness invariants by attaching apartness constraints to the type indices used in the definitions of data structures and functions. Consider the type indices for the two (user-defined) data structures used by dedup, linked lists and hash tries. The invariants expressed in the types are also useful for many other functional algorithms.

The programmer defines List and ListNode recursively, giving a reference cell at the head of each list and recursive sub-list (Fig. 2, right). Though not shown, TrieNode is defined similarly. The type indices enforce that, in each structure, each name appears at most once; but names may be shared across different structures.

In the type for Cons, the quantifier for name sets \(X_1\) and \(X_2\) includes the constraint \(X_1 \perp X_2\), which says that \(X_1\) and \(X_2\) are apart (disjoint). These indices appear in the types of the Cons cell’s name \((X_1)\), and its list tail \((X_2)\). Consequently, to form lists inductively, the constraint \(X_1 \perp X_2\) must hold, showing that each additional Cons cell name is distinct from the others already in its tail.

The type indices for insert are similar to those of Cons. They express a similar function in terms of name sets: stating that the resulting structure (a trie) contains an additional name (in \(X_1\)) not present in the input structure (name set \(X_2\)). The type for Nil allows any name set (a safe overapproximation), since Nil contains no concrete names at runtime. Similarly, the type for an empty trie (not shown) allows any name set.

Turning to the type signature of dedup, it includes the apartness constraint \(X_1 \perp X_2\), encoding the invariant that the type indices for dedup’s input structures (name sets \(X_1\) and \(X_2\)) are apart. The codomain of the type, List\{\(X_1\)\}, says that the resulting list contains the same names as the input list. The type system uses the apartness constraints within the types of Cons and insert to show that dedup’s apartness constraint holds for the recursive invocation of dedup.

Intuitively, that invocation moves name \(x (x = n_2\) in Fig. 3) from the head of input list 1 to the accumulated trie \(tx\), maintaining the pairwise apartness of names in each of the two structures. In terms of Fig. 3, the inductive reasoning about dedup’s invariants goes as follows. By assumption, the name sets of 1 and 2 are apart. (In Fig. 3, the name set of 1 is \{\(n_2\), \(n_3\), \(n_4\)\}, and the name set of
t is \{n_1\}.) In the Cons branch, the apartness constraint in the type signature for Cons provides that the name x at the Cons cell is apart from the names of the list tail ys, if any. (In Fig. 3, recall that x = n_2, and the names in ys consist of n_3 and n_4.) The type signature for insert provides that the names of the output trie consist of the existing names from the existing trie, along with the new name for the inserted element. In Fig. 3, the inserted trie tx contains the names n_1 and n_2.

Putting these facts together, in the recursive invocation of thunk ddys, we have that the names of the list tail ys (n_3 and n_4) and those of the updated trie tx (n_1 and n_2) are apart.

**Static reasoning:** To statically enforce both global and local uniqueness, Fungi uses decision procedures to determine whether (static approximations of) name sets are apart. When it needs to prove such an assertion, but decides otherwise, it tells the programmer that the name sets in question—describing either global effects or local type indices—cannot be proven to be apart. For instance, if the programmer mistakenly passed 1 instead of ys in the recursive call, the inductive invariant would not hold: the names of 1 and tx overlap at name x. As a result, Fungi would report that it cannot show the invariant for the recursive call.

Below, we consider insert in more depth (Sec. 2.5) before exploring other possible uniqueness errors within dedup (Sec. 2.6),

### 2.5 Helper function insert

Fig. 4 shows the Fungi programmer’s implementation of insert, in terms of a recursive function insrec (right column). The left column gives the type definition of TrieNode, whose use of indices is similar to ListNode from Fig. 2. Below this definition, the programmer defines various name and index terms, culminating in the definition of Insrec, which gives the write set for insert, just as Dedup did for dedup in Fig. 2.

Recall that dedup used structural recursion over a list with a name at each recursive position (Cons cell). Here, insrec illustrates a pattern of naming allocations within general recursion. The insert function takes a name, an element (natural number) and a trie; it returns the hash trie obtained by hashing the given element and inserting it into the given trie. In addition to the updated trie, insert returns a boolean indicating whether the element was already present in the trie (but with a distinct name). For clarity, we discuss a simpler variant that only returns the updated trie; the other variant is similar, with similar allocation effects.
To allocate a new trie path, the Fungi programmer uses names to identify each allocation. Rather than use names from an input structure, as with the structural recursion of dedup, $\text{insrec}$ generates name sets (statically) with Kleene closure: repeated application of a name function $\text{Succ}^*(x)$ to an initial set (Fig. 4). By defining write sets in this way, we can name any allocations within general recursion based on each allocation’s (complete) path in the recursive call graph. Since $\text{insrec}$ recurs only once, there is a single chain of calls and a natural number suffices to name each call.

The implementation of $\text{insrec}$ (dynamically) computes the sequence of names, starting from $\text{Zero}$. (As Fig. 3 illustrates, the last computed name corresponds to 4.) In the final iteration, $\text{insrec}$ creates a leaf node holding the inserted element $y$, and its associated name $x$. In a more complex structure, we would handle hash collisions by creating linked lists at these leaf positions; for simplicity, we assume here that hash collisions are impossible.

The index function $\text{Gte}$ gives the inductive invariant for $\text{insrec}$: Every numeral suffix written by the recursive call to $\text{insrec}$ is greater than the one written by the current iteration of the loop, $\pi\ell$. Recursive iterations will use $\pi\ell\cdot\pi\ell$, or some larger numeral. While natural numbers are not built-in to Fungi’s type index system, the programmer encodes the “greater than” constraint using Fungi’s notion of apartness.

### 2.6 Apartness failures violate global uniqueness

As explained above, Fungi enforces global uniqueness and local uniqueness by statically reasoning about apartness. In writing dedup without the Fungi type system, it is easy to make naming mistakes that violate an apartness constraint—breaking local uniqueness, global uniqueness, or both.

In Table 2, we list three classes of naming mistakes, showing concrete examples in the context of dedup and the apartness constraint that does not hold ($\not\models$). We explain each mistake in more detail, to see why it violates apartness, sometimes on very specific (and unlikely) inputs. It is easy to overlook these mistakes; the authors have made all of them.

To see the problem with a missing tag, consider mapping the name set $\{0, 0 \cdot 1\}$ by $\text{id}$ (the identity function) and by $\lambda x. x \cdot 1$: The images overlap on name $0 \cdot 1$, since the two names in the input set are already related by the second function $\lambda x. x \cdot 1$, which $\text{id}$ fails to distinguish by adding any tag of its own. By contrast, consider mapping the same name set by two apart name functions, $\lambda x. x \cdot 0$ and $\lambda x. x \cdot 1$: the two images are disjoint ($\{0 \cdot 0, (0 \cdot 1) \cdot 0\} \not\models (0 \cdot 1, (0 \cdot 1) \cdot 1)$).

To see the problem with prefix/suffix mismatches, consider mapping the name set $\{0, 1\}$ by $\lambda x. x \cdot 0$ and $\lambda x. x \cdot 1$: the two images overlap on name $0 \cdot 1$, since the two functions disagree about how they distinguish names in the input set.

Finally, to see the problem with what we call "overlapping primes", consider mapping the name set $\{0, 1\}$ by $\text{Succ}$ and $\text{Succ} \circ \text{Succ}$: the images overlap at name 2. The problem is similar to the missing tag problem, but at the level of name sets. Overlapping primes may involve Kleene closure, e.g., $X : \text{NmSet} \not\models \text{Succ}^*(\text{Succ}(X)) \perp X$. There is a critical difference between this apartness violation and the apartness property used by $\text{insrec}$ and $\text{insrec}$ in Sec. 2.5, $x : \text{Nm} \models \text{Succ}^*((\text{Succ}(x))) \perp [x]$. Like the violation above, this valid apartness property also involves Kleene closure, but the “seed”

<table>
<thead>
<tr>
<th>class of mistake</th>
<th>the dedup programmer...</th>
<th>apartness failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>missing tag</td>
<td>forgets $\oplus d$ and/or $\oplus r$</td>
<td>$\not\models \lambda x. (\oplus d \cdot x) \perp 1\oplus d$ and $\not\models \lambda x. (\oplus r \cdot x) \perp 1\oplus d$</td>
</tr>
<tr>
<td>prefix/suffix mismatch</td>
<td>uses $\oplus r$ as suffix, or forgets $\oplus t$</td>
<td>$\not\models \lambda x. (\oplus d \cdot x) \perp \lambda x. (\oplus t \cdot x)$</td>
</tr>
<tr>
<td>“overlapping primes”</td>
<td>defines $\text{Insrec} \ x = \text{Succ}^*x$</td>
<td>$X : \text{NmSet} \not\models \text{Succ}(\text{Succ}(X)) \perp \text{Succ}(X)$</td>
</tr>
</tbody>
</table>

Table 2. Naming mistakes, with examples from dedup and their associated apartness failure
When global uniqueness holds, the outcome of change propagation for any iteration is always correct. Change propagation, described in detail below, attempts to exploit these similarities to reuse past work wherever possible.

For example, priming the variable $A$ in the set $\{A, B, A'\}$ clashes with the existing $A'$.

### 2.7 Global uniqueness implies correct change propagation

The metatheory of the Fungi type system considers one run at a time. Within each run, it ensures global uniqueness, the prerequisite for change propagation to ensure from-scratch consistency: When global uniqueness holds, the outcome of change propagation for any iteration is always consistent with the outcome of a from-scratch run on the current input.

Using names to compare similar from-scratch runs. Because change propagation is from-scratch consistent, we can predict its time complexity (and other dynamic behavior) by comparing two from-scratch runs and seeing where they differ. Due to their use of names, the two runs similarities and differences can be identified precisely, by name. Change propagation, described in detail below, attempts to exploit these similarities to reuse past work wherever possible.

Fig. 5 shows two full runs of dedup on (similar) input lists $[3, 4, 3, 9]$ (left side) and $[1, 4, 3, 9]$ (right side).

The later recursive calls depend on the trie paths allocated in earlier calls. For instance, by carefully comparing the left and right runs’ allocated trie paths rooted at $\text{t} \cdot n_1 \cdot 0$, we see that the hashes of 3 and 1 consist of inverted bits: all of the pointers have “flipped” between left and right. Moving downward in the figure, the allocated trie paths rooted at $\text{t} \cdot n_2 \cdot 0$ differ at that name, and at $\text{t} \cdot n_2 \cdot 1$, but then “sync up” at $\text{t} \cdot n_2 \cdot 2 \rightarrow \text{t} \cdot n_2 \cdot 4$. The allocated trie paths rooted at $\text{t} \cdot n_3 \cdot 0$ and $\text{t} \cdot n_4 \cdot 0$ are the same in the two runs.
Because of the input list’s logical position names \((n_1 - n_4)\), the output list uses identical addresses in the left- and right-hand runs, where they overlap. The right-hand run’s list contents are similar, with three (necessary) exceptions: (a) the element at logical position \(n_1\) is changed to 1; (b) 3 appears at logical position \(n_3\) (and pointer name \(r \cdot n_3\)), whereas the left-hand run had a duplicate 3 at position \(n_3\); (c) the tail pointer in the output Cons cell \(r \cdot n_2\) differs, since position \(n_3\) was absent in the left-hand run.

**Change propagation.** Fig. 6 considers the behavior of using change propagation where the left run of Fig. 5 happens first, followed by an input change (at \(a_1\)), that precipitates change propagation updating this dependence graph to be from-scratch consistent with the right run. As explained above, the two runs in Fig. 5 differ at certain allocated names; change propagation selectively re-executes thunks in the dependence graph in an order that is consistent with a from-scratch run on the current input (in this case, the right run of Fig. 5). We indicate the re-executed thunks with an additional (blue) border pattern.

Change propagation re-executes thunk **comp** first, since it observes the changed input list cell \(a_1\) that replaces the first 3 with 1. As described above, the new element 1 hashes differently, resulting in a different pattern of pointers in this trie path rooted at \(t \cdot n_1 \cdot 0\).

We indicate overwritten (and changed) reference cells with an additional (red) border pattern. Fungi dynamically records thunks that depend on changed reference cells, and avoids reusing their results without first applying the change propagation algorithm to their dependence graphs. For this reason, change propagation next re-executes **dd \cdot n_1**.
Values 

\[ v ::= x \mid () \mid (v_1, v_2) \mid \text{inj}_i v \mid \text{name} n \mid \text{nmfn} M \mid \text{ref} n \mid \text{thunk} n \mid \text{pack}(a. v) \]

Terminal exprs. 

\[ t ::= \text{ret}(v) \mid \lambda x. e \]

Expressions 

\[ e ::= t \mid \text{split}(v, x_1.x_2.e) \mid \text{case}(v, x_1.e_1, x_2.e_2) \]

\[ \mid e v \mid \text{let}(e_1, x.e_2) \mid \text{thunk}(v, e) \mid \text{force}(v) \mid \text{ref}(v, v) \mid \text{get}(v) \]

\[ \mid \text{scope}(v, e) \mid v. M \mid \text{vunpack}(v, a. x. e) \]

Fig. 7. Syntax of expressions

When re-executed, \( \text{dd} \cdot n_1 \) changes some trie names with its overwrites, but not all of them (as described above). Next, it re-forces \( \text{dd} \cdot n_2 \), which re-executes (due to the trie overwrites).

When a re-execution results in behavior that is the same as the prior run, the frontier of change propagation may end, as with thunk \( \text{dd} \cdot n_2 \). Its allocations overwrite the prior reference cells with identical values. It (re-)forces \( \text{dd} \cdot n_3 \), whose local effects are unaffected by the input change (either directly or indirectly). In this case, Fungi reuses the cached result of this (unaffected) thunk.

Next, control returns to \( t \cdot n_1 \cdot 0 \), which overwrites its output cell’s tail pointer with the inserted (and new) cell at \( r \cdot n_3 \). Finally, control returns to \( \text{comp} \), which overwrites \( r \cdot n_1 \) with the changed input value 1, but returns the same result, \( r \cdot n_1 \). If \( \text{comp} \) were occurring in the context of more recursive calls in a longer input list, these earlier calls would be unaffected, and not re-executed.

In summary, the change propagation behavior described above critically relies on (unique) names to bring the initial and updated runs into a correspondence that it can efficiently exploit. Unique names are generally necessary for efficient (stable) change propagation, but not alone sufficient. In particular, the Fungi type-and-effect system enforces global uniqueness by reasoning about a single from-scratch execution, not the relationship between two (or more) similar executions on similar inputs. In Sec. 8, we discuss connections to (relational) cost semantics for incremental computation.

3 PROGRAM SYNTAX

The examples from the prior section use an informally defined variant of ML, enriched with a (slightly simplified) variant of our proposed type system. In this section and the next, we focus on a core calculus for programs and types, and on making these definitions precise.

3.1 Values and Expressions

Fig. 7 gives the grammar of values \( v \) and expressions \( e \). We use call-by-push-value (CBPV) conventions in this syntax, and in the type system that follows. There are several reasons for this. First, CBPV can be interpreted as a “neutral” evaluation order that includes both call-by-value or call-by-name, but prefers neither in its design. Second, since we make the unit of memoization a thunk, and CBPV makes explicit the creation of thunks and closures, it exposes exactly the structure that we extend to a general-purpose abstraction for incremental computation. In particular, thunks are the means by which we cache results and track dynamic dependencies.

Values \( v \) consist of variables, the unit value, pairs, sums, and several special forms (described below).

We separate values from expressions, rather than considering values to be a subset of expressions. Instead, terminal expressions \( t \) are a subset of expressions. A terminal expression \( t \) is either \( \text{ret}(v) \)—the expression that returns the value \( v \)—or a \( \lambda \). Expressions \( e \) include terminal expressions, elimination forms for pairs, sums, and functions (split, case and \( e v \), respectively); let-binding (which evaluates \( e_1 \) to \( \text{ret}(v) \) and substitutes \( v \) for \( x \) in \( e_2 \)); introduction (thunk) and elimination
Fungi: Typed incremental computation with names

\begin{align*}
\text{Names} & \quad m, n \ ::= \text{leaf} & \quad \text{leaf name} \\
\text{(binary trees)} & \quad | \langle\langle n_1, n_2 \rangle\rangle & \quad \text{binary name composition} \\
\text{Name terms} & \quad M, N \ ::= n \mid \langle\langle M_1, M_2 \rangle\rangle & \quad \text{literal names, binary name composition} \\
\text{(STLC+names)} & \quad | a \mid \lambda a. M \mid M(N) & \quad \text{variable, abstraction, application} \\
\text{Name term values} & \quad V \ ::= n \mid \lambda a. M & \quad \text{name; inhabitants n} \\
\text{Name term sorts} & \quad \gamma \ ::= N m & \quad \text{name term function; inhabitants } \lambda a. M \\
\text{Typing contexts} & \quad \Gamma \ ::= \cdot \mid \Gamma, a : \gamma & \quad \text{full definition in Figure 11} \\
\end{align*}

Fig. 8. Syntax of name terms: a \(\lambda\)-calculus over names, as binary trees

\[
\begin{array}{c}
\Gamma \vdash M : \gamma \\
\hline
\text{M-const} \\
\Gamma \vdash n : N m \\
\hline
\text{M-var} \\
\Gamma \vdash a : \gamma \\
\hline
\text{M-bin} \\
\Gamma \vdash \langle\langle M_1, M_2 \rangle\rangle : N m \\
\hline
\text{M-app} \\
\Gamma \vdash (\langle\langle M_1, M_2 \rangle\rangle) : N m \\
\hline
\end{array}
\]

Fig. 9. Sorting and evaluation rules for name terms \(M\)

(force) forms for thunks; and introduction (ref) and elimination (get) forms for pointers (reference cells that hold values).

The special forms of values are names name \(n\), name-level functions \(nmfn\) \(M\), references (pointers), and thunks. References and thunks include a name \(n\), which is the name of the reference or thunk, not the contents of the reference or thunk.

This syntax is similar to Adapton [Hammer et al. 2015]; we add the notion of a name function, which captures the idea of a namespace and other transformations on names. The scope \((v, e)\) construct controls monadic state for the current name function, composing it with a name function \(v\) within the dynamic extent of its subexpression \(e\). Name function application \(M \ v\) permits programs to compute with names and name functions that reside within the type indices. Since these name functions always terminate, they do not affect a program’s termination behavior.

We do not distinguish syntactically between value pointers (for reference cells) and thunk pointers (for suspended expressions); the store maps pointers to either of these.

### 3.2 Names

Figure 8 shows the syntax of literal names, name terms, name term values, and name term sorts. Literal names \(m, n\) are simply binary trees: either an empty leaf \(\text{leaf}\) or a branch node \(\langle\langle n_1, n_2 \rangle\rangle\). Name terms \(M, N\) consist of literal names \(n\) and branch nodes \(\langle\langle M_1, M_2 \rangle\rangle\), abstraction \(\lambda a. M\) and application \(M(N)\).

Name terms are classified by sorts \(\gamma\): sort \(N m\) for names \(n\), and \(\gamma \xrightarrow{\text{Nm}} \gamma\) for (name term) functions.

\[ \text{teval-value} \quad V \downarrow_M V \quad \text{teval-bin} \quad \langle\langle M_1, M_2 \rangle\rangle \downarrow_M \langle\langle n_1, n_2 \rangle\rangle \quad \text{teval-app} \quad M(N) \downarrow_M V' \]

, Vol. 1, No. 1, Article . Publication date: May 2021.
The structure of our type system is inspired by Dependent ML [Xi and Pfenning 1999; Xi 2007]. While disjoint union is common in the types of names. We write \( NmSet \) for the singleton name set, \( \emptyset \) for the empty name set, and \( X \perp Y \) for a union of two sets \( X \) and \( Y \) that requires \( X \) and \( Y \) to be disjoint; this is inspired by the separating conjunction of separation logic [Reynolds 2002]. While disjoint union is common in the types

4 TYPE SYSTEM

The structure of our type system is inspired by Dependent ML [Xi and Pfenning 1999; Xi 2007]. Unlike full dependent typing, DML is separated into a program level and a less-powerful index level. The classic DML index domain is integers with linear inequalities, making type-checking decidable. Our index domain includes names, sets of names, and functions over names. Such functions constitute a tiny domain-specific language that is powerful enough to express useful transformations of names, but preserves decidability of type-checking.

Indices in DML have no direct computational content. For example, when applying a function on vectors that is indexed by vector length, the length index is not directly manipulated at run time. However, indices can indirectly reflect properties of run-time values. The simplest case is that of an indexed singleton type, such as \( \text{Int}[k] \). Here, the ordinary type \( \text{Int} \) and the index domain of integers are in one-to-one correspondence; the type \( \text{Int}[3] \) has one value, the integer 3.

While indexed singletons work well for the classic index domain of integers, they are less suited to names—at least for our purposes. Unlike integer constraints, where integer literals are common in types—for example, the length of the empty list is 0—literal names are rare in types. Many of the name constraints we need to express look like “given a value of type \( A \) whose name in the set \( X \), this function produces a value of type \( B \) whose name is in the set \( f(X) \)”. A DML-style system can express such constraints, but the types become verbose:

\[
\forall a : \text{Nm}. \quad \forall X : \text{NmSet}. \quad (a \in X) \supset (A[a] \rightarrow B[f(a)]).
\]

The notation is taken from one of DML’s descendants, Stardust [Dunfield 2007]. The type is read “for all names \( a \) and name sets \( X \), such that \( a \in X \), given some \( A[a] \) the function returns \( B[f(a)] \).”

We avoid such locutions by indexing single values by name sets, rather than names. For types of the shape given above, this removes half the quantifiers and obviates the \( \epsilon \)-constraint attached via \( \supset \): \( \forall X : \text{NmSet}. \quad A[X] \rightarrow B[f(X)] \). This type says the same thing as the earlier one, but now the approximations are expressed within the indexing of \( A \) and \( B \). Note that \( f \), a function on names, is interpreted pointwise: \( f(X) = \{ f(N) \mid N \in X \} \). Standard singletons are handy for index functions on names, where one usually needs to know the specific function.

For aggregate data structures such as lists, indexing by a name set denotes overapproximation of names: the proper DML type \( \forall Y : \text{NmSet}. \quad \forall X : \text{NmSet}. \quad (Y \subseteq X) \supset (A[Y] \rightarrow B[f(Y)]) \) can be expressed by \( \forall X : \text{NmSet}. \quad A[X] \rightarrow B[f(X)] \).

Following call-by-push-value [Levy 1999, 2001], we distinguish value types from computation types. Our computation types will also model effects, such as the allocation of a thunk with a particular name.

4.1 Index Level

Figure 10 gives the syntax of index expressions and index sorts (which classify indices). We use several meta-variables for index expressions; by convention, we use \( X, Y, Z, R \) and \( W \) only for sets of names—index expressions of sort \( \text{NmSet} \).

Name sets. If we give a name to each element of a list, then the entire list should carry the set of those names. We write \( \{ N \} \) for the singleton name set, \( \emptyset \) for the empty name set, and \( X \perp Y \) for a union of two sets \( X \) and \( Y \) that requires \( X \) and \( Y \) to be disjoint; this is inspired by the separating conjunction of separation logic [Reynolds 2002]. While disjoint union is common in the types
### Index expressions

| i, j | ::= | a | index variable |
| X, Y, Z | | \{N\} | singleton name set |
| R, W | | \emptyset | X \perp Y | empty set, separating union |
| | | X \cup Y | union (not necessarily disjoint) |
| | | \{i, i\} | prj_1 i | prj_2 i | unit, pairing, and projection |
| | | \lambda a. i | i(j) | function abstraction and application |
| | | M[i] | i[j] | name set mapping and set building |

### Index sorts

\[ \gamma ::= \cdots | \text{NmSet} \]

- unit index sort; inhabitant \( \emptyset \)
- product index sort; inhabitants \((i, j)\)
- index functions over name sets

### Kinds

\[ K ::= \text{type} \]

- kind of value types
- type argument (binder space)
- index argument (binder space)

### Propositions

\[ P ::= \text{tt} | P \land P \]

- truth and conjunction
- index apartness
- index equivalence

### Effects

\[ \epsilon ::= (W; R) \]

### Value types

\[ A, B ::= \alpha | d | \text{unit} \]

- type variables, type constructors, unit
- sum, product
- named reference cell
- named thunk (with effects)
- application of type to index
- application of type constructor to type
- name type (name in name set \( i \))
- name function type (singleton)
- universal index quantifier
- existential index quantifier

### Computation types

\[ C, D ::= \text{F} A | A \to E \]

- \text{iFt}, functions

### Typing contexts

\[ \Gamma ::= \]

- index variable sorting
- type variable kinding
- type constructor kinding
- ref pointer
- thunk pointer
- value variable
- proposition \( P \) holds

---

that we believe programmers need, our effects discipline requires non-disjoint union \( X \cup Y \), so we include it as well.
Variables, pairing, functions. An index $i$ (also written $X$, $Y$, … when the index is a set of names) is either an index-level variable $a$, a name set (described above: \{N\}, $X \perp Y \text{ or } X \cup Y$), the unit index $\emptyset$, a pair of indices $(i_1, i_2)$, pair projection $\text{pr}_b i$ for $b \in \{1, 2\}$, an abstraction $\lambda a. i$, application $i[j]$, or name term application $M[i]$.

Name terms $M$ are not a syntactic subset of indices $i$, though name terms can appear inside indices (for example, singleton name sets $\{M\}$). Because name terms are not a syntactic subset of indices (and name sets are not name terms), the application form $i[j]$ does not allow us to apply a name term function to a name set. Thus, we also need name term application $M[i]$, which applies the name function $M$ to each element of the name set $i$. The index-level map form $i[j]$ collects the output sets of function $i$ on the elements of the input set $j$. The Kleene star variation $i^*[j]$ applies the function $i$ zero or more times to each input element in set $j$.

Sorts. We use the meta-variable $\gamma$ to classify indices as well as name terms. We inherit the function space $\text{Nm}$ from the name term sorts (Figure 8). The sort $\text{NmSet}$ (Figure 10) classifies indices that are name sets. The function space $\text{Nm}$ classifies functions over indices (e.g., tuples of name sets), not merely name terms. The unit sort and product sort classify tuples of index expressions.

Most of the sorting rules in Figure 12 are straightforward, but rule ‘sort-sep-union’ includes a premise $\text{extract}(\Gamma) \vdash X \perp Y : \text{NmSet}$, which says that $X$ and $Y$ are apart (disjoint).

Propositions and extraction. Propositions $P$ are conjunctions of atomic propositions $i \equiv j : \gamma$ and $i \perp j : \gamma$, which express equivalence and apartness of indices $i$ and $j$. For example, $\{n_1\} \perp \{n_2\} : \text{NmSet}$ implies that $n_1 \neq n_2$. Propositions are introduced into $\Gamma$ via index polymorphism $\forall a : \gamma \mid P$, $E$, discussed below.

The function $\text{extract}(\Gamma)$ (Figure 28 in the appendix) looks for propositions $P$, which become equivalence and apartness assumptions. It also translates $\Gamma$ into the relational context used in the definition of apartness. We give semantic definitions of equivalence and apartness in the appendix (Definitions F.6 and F.7).
Under assumptions \(\Gamma\), value \(v\) has type \(A\):
\[
\Gamma \vdash v : A
\]

\(\Gamma \vdash x : A\)
\(\Gamma \vdash \text{pack}(a,v) : (\forall a : \gamma \mid P,A)\)

\subsection{Kinds}

We use a simple system of *kinds* \(K\) (Figure 21 in the appendix). Kind type classifies value types, such as unit and \((\text{Thk}[i] \mid \varnothing)\).

Kind type \(\Rightarrow K\) classifies type expressions that are parametrized by a type. Such types are called *type constructors* in some languages.

Kind \(\gamma \Rightarrow K\) classifies type expressions parametrized by an index. For example, the List type constructor from Section 2 takes a name set: List[X], so List has kind \(\text{NmSet} \Rightarrow \text{type}\). A more general Seq type would also track its pointers (not just its names), and permit any element type, and would thus have kind \(\text{NmSet} \Rightarrow (\text{NmSet} \Rightarrow (\text{type} \Rightarrow \text{type}))\).

\subsection{Effects}

Effects are described by \((W,R)\), meaning that the associated code may write names in \(W\), and read names in \(R\). (To simplify the example in the overview, we omitted the read set.)

Effect sequencing (Figure 14) is a (meta-level) partial function over a pair of effects: the judgment \(\Gamma \vdash e_1\) then \(e_2 = e\), means that \(e\) describes the combination of having effects \(e_1\) followed by effects \(e_2\). Sequencing is a partial function because the effects are only valid when (1) the writes of \(e_1\) are disjoint from the writes of \(e_2\), and (2) the reads of \(e_1\) are disjoint from the writes of \(e_2\). Condition (1) holds when each cell or thunk is not written more than once (and therefore has a unique value). Condition (2) holds when each cell or thunk is written before it is read.

Effect coalescing, "\(E \text{ after } e\)”, combines "clusters" of effects: \((C \triangleright (\{n_2\};\emptyset)) \text{ after } (\{n_1\};\emptyset) = C \triangleright ((\{n_1\};\emptyset) \text{ then } (\{n_2\};\emptyset)) = C \triangleright (\{n_1,n_2\};\emptyset)\). Effect subsumption \(e_1 \leq e_2\) holds when the write and read sets of \(e_1\) are subsets of the respective sets of \(e_2\).
Effect sequencing

\[ \Gamma \vdash (\epsilon_1 \text{ then } \epsilon_2) = \epsilon \]

Effect coalescing

\[ \Gamma \vdash (E \text{ after } \epsilon) = E' \]

Effect subsumption

\[ \Gamma \vdash (X_1 \downarrow Z_1) \equiv Y_1 : \text{NmSet} \]
\[ \Gamma \vdash (X_2 \downarrow Z_2) \equiv Y_2 : \text{NmSet} \]

\[ \Gamma \vdash (X_1; X_2) \leq (Y_1; Y_2) \]

Under \( \Gamma \), within namespace \( M \), computation \( \epsilon \) has type-with-effects \( E \)

\[ \Gamma, x_1 : A_1, x_2 : A_2 \vdash M \vdash e : E \]

\[ \Gamma \vdash (\lambda x. e) : ((A \rightarrow E) \rightarrow (\emptyset; \emptyset)) \]

\[ \Gamma \vdash : \text{Nm}[X] \]

\[ \Gamma \vdash \text{thunk}(\epsilon) : (F(\text{Thk}[M[X]]E)) \rightarrow (M[X]; \emptyset) \]

\[ \Gamma \vdash : \text{Nm}[\text{[M]}] \]

\[ \Gamma \vdash \text{force}(\epsilon) : (C \triangleright \epsilon') \]

\[ \Gamma \vdash \text{ref}(\epsilon_1, \epsilon_2) : F [\text{Ref}[M[X]]A] \rightarrow (M[X]; \emptyset) \]

\[ \Gamma \vdash : \text{Nm}[\text{Nm}[\text{[M]]]} \]

\[ \Gamma \vdash : \text{Nm}[\text{Nm}[\text{Nm}[\text{[M]]]}] \rightarrow (\emptyset; \emptyset) \]
4.4 Types
The value types (Figure 11), written $A$, $B$, include standard sums $+$ and products $\times$; a unit type; the type $\text{Ref}[i]A$ of references named $i$ containing a value of type $A$; the type $\text{Thk}[i]E$ of thunks named $i$ whose contents have type $E$ (see below); the application $A[i]$ of a type to an index; the application $A \circ B$ of a type $A$ (e.g. a type constructor $d$) to a type $B$; the type $\text{Nm}[i]$; and a singleton type $(\text{Nm} \Rightarrow \text{Nm})[M]$ where $M$ is a function on names.

As usual in call-by-push-value, computation types $C$ and $D$ include a connective $F$, which "liFts" value types to computation types: $FA$ is the type of computations that, when run, return a value of type $A$. (Call-by-push-value usually has a connective dual to $F$, written $U$, that "thUnks" a computation type into a value type; in our system, $\text{Thk}$ plays the role of $U$.)

Computation types also include functions, written $A \rightarrow E$. In standard CBPV, this would be $A \rightarrow C$, not $A \rightarrow E$. We separate computation types alone, written $C$, from computation types with effects, written $E$; this decision is explained in Appendix A.3.

Computation types-with-effects $E$ consist of $C \triangleright \epsilon$, which is the bare computation type $C$ with effects $\epsilon$, as well as universal quantifiers (polymorphism) over types ($\forall \alpha : K. E$) and indices ($\forall \alpha : \gamma | P. E$). In the latter quantifier, the proposition $P$ lets us express quantification over disjoint sets of names.

Value typing rules. The typing rules for values (Figure 13) for unit, variables and pairs are standard. Rule 'name' uses index-level entailment to check that the name $n$ is in the name set $X$. Rule 'namefn' checks that $Mv$ is well-sorted, and that $Mv$ is convertible to $Mv$. Rule 'ref' checks that $n$ is in $X$, and that $\Gamma(n) = A$, that is, the typing $n:A$ appears somewhere in $\Gamma$; rule 'thunk' is similar.

Computation typing rules. Many of the rules that assign computation types (Figure 14) are standard—for call-by-push-value—with the addition of effects and the namespace $M$. The rules 'split' and 'case' have nothing to do with namespaces or effects, so they pass $M$ up to their premises, and leave the type $E$ unchanged. Empty effects are added by rules 'ret' and 'lam', since both ret and $\lambda$ do not read or write anything. The rule 'let' uses effect sequencing to combine the effects of $e_1$ and the let-body $e_2$. The rule 'force' also uses effect sequencing, to combine the effect of forcing the thunk with the read effect $\langle \emptyset; X \rangle$.

The only rule that modifies the namespace is 'scope', which composes the given namespace $N$ (in the conclusion) with the user's $v = \text{nmfn} N'$ in the second premise (typing $e$).

4.5 Subtyping
As discussed above, our type system can overapproximate names. The type $\text{Nm}[X]$ means that the name is contained in the set of $X$; unless $X$ is a singleton, the type system does not guarantee the specific name. Approximation induces subtyping: we want to allow a program to pass $\text{Nm}[X_1 \bot X_2]$ to a function expecting $\text{Nm}[X_1 \cap X_2]$.

For space reasons, the subtyping rules are given and explained in the appendix (Sec. A.1).

4.6 Bidirectional Version
The typing rules in Figures 13 and 14 are declarative: they define what typings are valid, but not how to derive those typings. The rules' use of names and effects annotations means that standard unification-based techniques, like Damas–Milner inference, are not readily applicable. For example, it is not obvious when to apply etype-\forall Intro, or how to solve unification constraints over names and name sets.

Bidirectional typing [Pierce and Turner 1998] alternates between checking an expression against a known type (e.g. from a type annotation) and synthesizing a type from an expression. Since
checking rules utilize the given type, bidirectional typing is decidable for a wide range of rich type systems; see the citations in Dunfield and Krishnaswami [2013]. Therefore, we formulate bidirectional typing rules that are decidable and directly give rise to an algorithm.

For space reasons, this system is presented in the supplementary material (Appendix C). We prove in Appendix D that our bidirectional rules are sound and complete with respect to the type assignment rules in this section:

Soundness (Thms. D.1, D.3): Given a bidirectional derivation for an annotated expression \( e \), there exists a type assignment derivation for \( e \) without annotations.

Completeness (Thms. D.2, D.4): Given a type assignment derivation for \( e \) without annotations, there exist two annotated versions of \( e \): one that synthesizes, and one that checks. (This result is sometimes called *annotatability*.)

5 DYNAMIC SEMANTICS

Name terms. Recall Fig. 9 (Sec. 3.2), which gives the dynamics for evaluating name term \( M \) to name term value \( V \). Because name terms have no recursion, evaluating a well-sorted name term always produces a value (Theorem G.9).

Program expressions (Figure 15). Stores hold the mutable state that names dynamically identify. Big-step evaluation for expressions relates an initial and final store, and the “current scope” and “current node”, to a program and value. We define this dynamic semantics, which closely mirrors prior work, to show that well-typed evaluations always allocate with unique names.

To make this theorem meaningful, the dynamics permits programs to *overwrite* prior allocations with later ones: if a name is used ambiguously, the evaluation will replace the old store content with the new store content. The rules \( \downarrow \text{-ref} \) and \( \downarrow \text{-thunk} \) either extend or overwrite the store, depending on whether the allocated pointer name is unique or ambiguous, respectively. We prove that, in fact, well-typed programs always extend (and never overwrite) the store in any single derivation. (During change propagation, not modeled here, we begin with a store and dependency graph from
Fungi: Typed incremental computation with names

a prior run, and even programs without naming errors overwrite the (old) store/graph, as discussed in Sec. 1.)

While motivated by incremental computation, we are interested in the allocation effects of a single run, not change propagation between runs. Consequently, this semantics is simpler than the dynamics of prior work. First, the store never caches values from evaluation, that is, it does not model function caching (memoization). Next, we do not build the dependency edges required for change propagation. Likewise, the “current node” is not strictly necessary here, but we include it for illustration. Were we modeling change propagation, rules ⇓-ref, ⇓-thunk, ⇓-get and ⇓-force would create dependency edge structure that we omit here. (These edges relate the current node with the node being observed.)

6 METATHEORY: TYPE SOUNDNESS AND UNIQUE NAMES

In this section, we prove that our type system is sound with respect to evaluation: Every well-typed, terminating program produces a terminal computation of the program’s type, the set of dynamic allocations match the program’s static approximation, and each allocation is globally unique. Def. 6.2 defines which evaluation derivations have precise effects matching the requirements above.

We sometimes constrain typing contexts to be store types, which type store pointers but not program variables; hence, they only type closed values and programs:

Definition 6.1 (Store type). We say that Γ is a store typing, written Γ store-type, when each assumption in Γ has the reference-pointer form p : A or the thunk-pointer form p : E.

Definition 6.2 (Precise effects). Given an evaluation derivation D, we write D reads R writes W for its precise effects (Figure 20 in the appendix).

This is a (partial) function over derivations. We call these effects “precise” since sibling sub-derivations must have disjoint write sets.

We write ⟨W′; R′⟩ ≤ ⟨W; R⟩ to mean that W′ ⊆ W and R′ ⊆ R. For proofs, see Appendix B.

Theorem 6.1 (Subject Reduction). If Γ1 store-type and Γ1 ⊢ M : Nm and Γ1 ⊢ M e : C ⊢ ⟨W; R⟩ and ⊲: S1 : Γ1 and D derives S1 ⊢ M e ⊲: S2; t then there exists Γ2 ⊇ Γ1 s.t. Γ2 store-type and ⊲: S2 : Γ2 and Γ2 ⊢ t : C ⊢ ⟨∅; ∅⟩ and D reads R and ⟨W2; R2⟩ ≤ ⟨W; R⟩.

Our implementation (Sec. 7) follows the change propagation algorithm of Hammer et al. [2015], which has been formalized and proven correct (from-scratch consistent) when Def. 6.2 (precise effects) holds for every program run under consideration—a guarantee of Fungi’s type-and-effect system, as stated above.

7 IMPLEMENTATION

7.1 Prototype in Rust

Using this on-paper design as a guide, we have implemented a preliminary prototype of Fungi in Rust. In particular, we implement each abstract syntax definition and typing judgement presented in this paper and appendix as a Rust datatype (a “deep” embedding of the language into Rust). We implement the bidirectional type system (Sec. C) as a family of Rust functions that produce judgement data structures (possibly with nested type or effect errors) from a Fungi syntax tree.

By using Rust macros, we implement a concrete syntax and associated parser that suffices for authoring examples similar to those in Sec. 2. In two ways, we deviate from the Fungi program syntax presented here: (1) Rust macros can only afford certain concrete syntaxes (2) Fungi programs use explicit (not implicit) index and type applications; inferring these arguments is future work.

We implement an incremental semantics for Fungi based on Adapton in Rust, as provided by an existing external library [Adapton Developers 2018]. This library uses the change propagation
algorithm(s) of Hammer et al. [2014, 2015]. The implementation of Fungi is documented and publicly available. At present, it consists of about 10K lines of Rust. For the latest version of Fungi, see crates.io and/or docs.rs, and search for “fungi-lang”. Note to reviewers: visiting those sites will deanonymize the authors; see supplemental material instead.

7.2 Ongoing and Future Work

Sec. 3 discusses a proposal for imperative (name) effects in the context of incremental sub-computations that (still) require unique names. Conceivably, future Fungi-based systems could track reactive names and their effects, potentially encoding reactive aspects of FRP language semantics [Elliott and Hudak 1997; Wan and Hudak 2000; Cooper and Krishnamurthi 2006; Krishnaswami and Benton 2011; Krishnaswami 2013; Czaplicki and Chong 2013]. In the long term, we intend Fungi as a target language for higher-level incremental programming languages.

Interactive type derivations. To debug the examples’ type and effect errors, we load the (possibly incomplete) typing derivations in an associated interactive, web-based tool. The tool makes the output typing derivation interactive: using a pointer, we can inspect the syntactic family/constructor, typing context, type and effect of each subterm in the input program, including indices, name terms, sorts, values, expressions, etc. Compared with getting parsing or type errors out of context (or else, only with an associated line number), we’ve found this interactive tool very helpful for teaching newcomers about Fungi’s abstract syntax rules and type system, and for debugging examples (and Fungi) ourselves. This tool, the Human-Fungi Interface (HFI), is publicly available software.

As future work, we will extend HFI into an interactive program editor, based on our existing bidirectional type system, and the (typed) structure editor approach developed by Omar et al. [2017a]. We speculate that Fungi itself may be useful in the implementation of this tool, by providing language support for interactive, incremental developer features [Omar et al. 2017b]. Current approaches prescribe conversion to a distinct, “co-contextual” judgement form that requires transforming the desired typing rules and their modes [Erdweg et al. 2015; Kuci et al. 2017]. Fungi’s explicit-name programming model may offer an alternative approach for authoring incremental type checkers, based on their “ordinary” judgments (rule and typing context structure).

8 RELATED WORK

DML [Xi and Pfenning 1999; Xi 2007] is an influential system of limited dependent types or indexed types. Inspired by Freeman and Pfenning [1991], who created a system in which datasort refinements were clearly separated from ordinary types, DML separates the “weak” index level of typing from ordinary typing; the dynamic semantics ignores the index level.

Motivated in part by the perceived burden of type annotations in DML, liquid types [Rondon et al. 2008; Vazou et al. 2013] deploy machinery to infer more types. These systems also provide more flexibility: types are not indexed by fixed tuples.

To our knowledge, Gifford and Lucassen [1986] were the first to express effects within (or alongside) types. Since then, a variety of systems with this power have been developed. A full accounting of this area is beyond the scope of this paper; for an overview, see Henglein et al. [2005]. We briefly discuss a type system for regions [Tofte and Talpin 1997], in which allocation is central. Regions organize subsets of data, so that they can be deallocated together. The type system tracks each block’s region, which in turn requires effects on types: for example, a function whose effect is to return a block within a given region. Our type system shares region typing’s emphasis on allocation, but we differ in how we treat the names of allocated objects. First, names in our system are fine-grained, in contrast to giving all the objects in a region the same designation. Second, names have structure—for example, the names 0-n = (leaf, n) and 1-n = (leaf, leaf, n)
share the right subtree $n$—which allows programmers to deterministically compute two distinct names from one.

Substructural type systems [O’Hearn 2003; Walker 2005] might seem suitable for statically verifying the correct usage of names. We initially believed that an affine type system would be good for checking global uniqueness, but we abandoned that route. First, sharing between data structures can be essential for efficiency (e.g. a `suffixes` function over a list). Second, while global uniqueness itself seems within the scope of affine typing, the justification for global uniqueness rests on local uniqueness properties that fall outside the scope of affine typing. It is conceivable that some not-yet-invented substructural type system could accomplish our goals, but “off-the-shelf” affine typing is not viable.

Type systems for variable binding and fresh name generation, such as FreshML [Pitts and Gabbay 2000] and Pure FreshML [Pottier 2007], can express that sets of names are disjoint. But the names lack internal structure that relates specific names across disjoint name sets.

Compilers have long used alias analysis to support optimization passes. Brandauer et al. [2015] extend alias analysis with disjointness domains, which can express local (as well as global) aliasing constraints. Such local constraints are more fine-grained than classic region systems; our work differs in having a rich structure on names.

**Approaches to incremental computation.** General-purpose incremental computation techniques use change propagation algorithms. Change propagation is a provably sound approach for recomputing the affected output, as the input changes dynamically after an initial run of the program [Acar et al. 2006b; Acar and Ley-Wild 2008; Hammer et al. 2014, 2015].

Our type and effect system complements past work on self-adjusting computation. In particular, we expect that variations of the proposed type system can express and verify the use of names in some of the work cited above.

Incremental computation can deliver asymptotic speedups for certain algorithms [Acar et al. 2007, 2008, 2009; Sümer et al. 2011; Chen et al. 2012], and has even addressed open problems [Acar et al. 2010]. Incremental computing abstractions exist in many settings [Shankar and Bodik 2007; Hammer et al. 2009; Acar and Ley-Wild 2008]. Cai et al. [2014] use derivatives in an incremental λ-calculus, which is more restricted than our setting (for example, their calculus lacks rich datatypes). Approaches such as concurrent revisions [Burckhardt et al. 2011], hybrid reactive/imperative programming [Demetrescu et al. 2011], and embedded incremental query languages [Mitschke et al. 2014] constitute alternate approaches to incremental computation, but diverge more markedly from conventional programming languages.

Çiçek et al. [2015] develop cost semantics for a limited class of incremental programs: they support only in-place input changes and fixed control flow, so that the structure of the dynamic dependency graph is fixed. For example, the length of an input list cannot change across successive incremental runs, nor can the structure of its dependency graph. Çiçek et al. [2016] relax the restriction on control flow (but not input changes) to permit replacing a dependency subgraph according to a different, from-scratch execution. Extending their cost semantics to allow general structural changes (e.g. insertion or removal of list elements), while describing the cost of change propagation for programs like `dedup` from Sec. 2, would require integrating a general notion of names. Without such a notion, constant-sized input changes may cascade, preventing reuse.

**Detection of naming errors.** Some past systems dynamically detect ambiguous names, either forcing the system to fall back to a non-deterministic name choice [Acar et al. 2006b; Hammer and Acar 2008], or to signal an error and halt [Hammer et al. 2015]. In scenarios with a non-deterministic fall-back mechanism, a name ambiguity carries the potential to degrade incremental performance, making it less responsive and asymptotically unpredictable in general [Acar 2005].
To ensure that incremental performance gains are predictable, past work often merely assumes, without enforcement, that names are precise [Ley-Wild et al. 2009]. These existing approaches are complementary to Fungi, whose type and effect system is applicable to each, either directly (in the case of Adapton, and variants), or with some minor adaptations (as we speculate for the others).

9 CONCLUSION

We present Fungi, a typed functional language for incremental computation with names. Unlike prior general-purpose languages for incremental computing (Table 1), Fungi’s notion of names is formal, general, and statically verified. In particular, Fungi’s type-and-effect system permits the programmer to encode (program-specific) local uniqueness invariants about names, and to use these invariants to establish global uniqueness for their composed programs, the property of using names correctly. We derive a bidirectional version of the type and effect system, and we have implemented a prototype of Fungi in Rust. We apply Fungi to a library of incremental collections.

Our ongoing and future work on Fungi builds on initial prototypes reported here: We are extending Fungi to settings that mix imperative and functional programming models, and we are creating richer tools for developing, debugging and visualizing Fungi programs in the context of larger systems (e.g., written in Rust).

ACKNOWLEDGMENTS

We thank Ryan L. Vandersmith, who leads the development of the Human-Fungi Interface described in Sec. 7; this tool has been invaluable for implementing and testing our Fungi prototype in Rust.

We thank Neelakantan R. Krishnaswami, Deepak Garg, Roly Perera, and David Walker for insightful discussions about this work, and for their suggestions and comments. This material is based in part upon work supported by a gift from Mozilla, a gift from Facebook, and support from the National Science Foundation under grant number CCF-1619282. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Mozilla, Facebook or the National Science Foundation.

REFERENCES


Value type $A$ is a subtype of $B$
\[
\frac{\Gamma \vdash A \leq_v B}{\Gamma \vdash A \leq_v A} \quad \leq_v \text{refl}
\]
\[
\frac{\Gamma \vdash A \leq_v B}{\Gamma \vdash A_1 \leq_v B_1} \quad \leq_v \text{x}
\]
\[
\frac{\Gamma \vdash A \leq_v B}{\Gamma \vdash A_1 \times A_2 \leq_v B_1 \times B_2} \quad \leq_v \text{x}
\]
\[
\frac{\Gamma \vdash A \leq_v B}{\Gamma \vdash \text{extract}(\Gamma) \leq_v \text{Ref}[X] A} \quad \leq_v \text{ref}
\]
\[
\frac{\Gamma \vdash A \leq_v B}{\Gamma \vdash \text{extract}(\Gamma) \leq_v \text{Ref}[Y] B} \quad \leq_v \text{ref}
\]
\[
\frac{\Gamma \vdash (\text{Ref}[X] A) \leq_v (\text{Ref}[Y] B)}{\Gamma \vdash (\text{Ref}[X] A) \times (\text{Ref}[Y] B) \leq_v (\text{Ref}[X] A) \times (\text{Ref}[Y] B)} \quad \leq_v \text{x}
\]
\[
\frac{\Gamma \vdash (\text{Thk}[X] E_1) \leq_v (\text{Thk}[Y] E_2)}{\Gamma \vdash (\text{Thk}[X] E_1) \leq_v (\text{Thk}[Y] E_2)} \quad \leq_v \text{thk}
\]

Computation type $C$ is a subtype of $D$
\[
\frac{\Gamma \vdash A \leq_v B}{\Gamma \vdash F A \leq_c F B} \quad \leq_c \text{lift}
\]
\[
\frac{\Gamma \vdash A_1 \leq_c A \quad \Gamma \vdash E_1 \leq E_2}{\Gamma \vdash (A_1 \rightarrow E_1) \leq_c (A_2 \rightarrow E_2)} \quad \leq_c \text{arr}
\]

Type-with-effects $E_1$ is a subtype of $E_2$
\[
\frac{\Gamma \vdash C \leq_c D}{\Gamma \vdash C_1 \leq C_2 \quad \Gamma \vdash e_1 \leq e_2}{\Gamma \vdash (C_1 :> e_1) \leq (C_2 :> e_2)} \quad \leq_e \text{eff}
\]
\[
\frac{\Gamma \vdash a : K \vdash E_1 \leq E_2}{\Gamma \vdash (\forall \alpha : K. E_1) \leq (\forall \alpha : K. E_2)} \quad \leq_e \text{all-type}
\]
\[
\frac{\Gamma \vdash i : \gamma}{\Gamma \vdash \text{extract}(\Gamma) \vdash [i/a]P} \quad \leq_e \text{all-name}
\]
\[
\frac{\Gamma \vdash (\forall \alpha : \gamma. P) \leq e_1 E_2}{\Gamma \vdash (\forall \alpha : \gamma. P) \leq e_1 E_2} \quad \leq_e \text{all-index-\text{L}}
\]
\[
\frac{\Gamma \vdash e_1 \leq E_2}{\Gamma \vdash (\forall \alpha : \gamma. P) \leq e_1 E_2} \quad \leq_e \text{all-index-\text{R}}
\]

Fig. 16. Subtyping on value types

Fig. 17. Subtyping on computation types

A  OMITTED DEFINITIONS, FIGURES, AND REMARKS

A.1 Subtyping

To design subtyping rules that are correct and easy to implement, we turn to the DML descendant Stardust [Dunfield 2007]. The subtyping rules in Stardust are generally a helpful guide, with the exception of the rule that compares atomic refinements. In Dunfield’s system, $\tau[i] \leq \tau[j]$ if $i = j$ in the underlying index theory. For example, a list of length $i$ is a subtype of a list of length $j$ if and only if $i = j$ in the theory of integers. While approximate in the sense of considering all lists of length $i$ to have the same type, the length itself is not approximate.
In contrast, our name set indices are approximations. Thus, our rule \( \leq_v \text{name} \) (Figure 16) says that \( \text{Nm}[X] \leq_v \text{Nm}[Y] \) if \( X \subseteq Y \), rather than \( X = Y \). Similarly, subtyping for references and thunks (\( \leq_v \text{-ref}, \leq_v \text{-thk} \)) checks inclusion of the associated name (pointer) set, not strict equality.

Our polymorphic types combine two fundamental typing constructs, universal quantification and guarded types (requiring that \( P \) hold for the quantified index \( a \)), so our rule \( \leq_v \text{-}\forall \) combines the Stardust rules \( \Pi L \) for index-level quantification and \( \supseteq L \) for the guarded type [Dunfield 2007, p. 33]. Likewise, our \( \leq_v \text{-}\forall R \) combines Stardust’s \( \Pi R \) and \( \supseteq R \).

Unlike Stardust’s \( \Sigma \) (and unlike our \( \forall \)), our existential types have a term-level pack construct, so an \( \exists \) cannot be a sub- or supertype of a non-existential type. Thus, instead of rules analogous to Stardust’s \( \Sigma L \) and \( \Sigma R \), we have a single rule \( \leq_v \exists \) with \( \exists \) on both sides, which specializes \( \Sigma R \) to the case when \( \Sigma L \) derives its premise. Like \( \forall \), our \( \exists \) incorporates a constraint \( P \) on the quantified variable, so our \( \leq_v \exists \) also incorporates the Stardust rules for asserting types (\( \exists P \)), checking that \( P_a \) entails \( P_b \).

For refs and thunks, rules \( \leq_v \text{-ref} \) and \( \leq_v \text{-thk} \) are covariant in the name set describing the location. They are also covariant in the type of their contents: unlike an ordinary ML ref type, our Ref names a location, but the programs described by our type system cannot mutate that location. To extend our theory to editor programs, we would need different rules (Section A.3 in the appendix).

In our subtyping rules for computation types (Figure 17), rule \( \leq_C \text{-arr} \) reflects the usual contravariance of function domains, rule \( \leq_E \text{-eff} \) allows subsumption within effects \( \epsilon \), and the rules for computation-level \( \forall \) follow our rules for value-level \( \forall \). Instead of an explicit transitivity rule, which is not trivial to implement, the transitivity of subtyping is admissible.

### A.2 Dynamic semantics, read and write sets, sorting and kinding

\[
\begin{align*}
\frac{\vdash \cdot : \Gamma \quad S \vdash \Gamma \quad \Gamma \vdash v : A \quad \Gamma(p) = A}{\vdash (S, p : v) : \Gamma} & \quad \text{ref} \\
\frac{\vdash \cdot : \Gamma \quad S \vdash \Gamma \quad \Gamma \vdash e : E \quad \Gamma(p) = E}{\vdash (S, p : e) : \Gamma} & \quad \text{thunk}
\end{align*}
\]

Fig. 18. Store typing: \( S \vdash \Gamma \), read “store S typed by \( \Gamma \)”.

In Figure 20, we write

\( \mathcal{D} \) by RuleName (\( \mathcal{D} \)list) reads \( R \) writes \( W \)

to mean that rule RuleName concludes \( \mathcal{D} \) and has subderivations \( \mathcal{D} \)list. For example,

\( \mathcal{D} \) by \( \downarrow \)-scope (\( \mathcal{D}_0 \)) reads \( R \) writes \( W \)

provided that \( \mathcal{D} \) reads \( R \) writes \( W \), where \( \mathcal{D}_0 \) derives the only premise of \( \downarrow \)-scope.
\[
\begin{align*}
\text{Pointers} & \quad p, q \ ::= \ n & \quad \text{name constants} \\
\text{Stores} & \quad S ::= & \quad \text{empty store} \\
& \quad | S, p: \nu & \quad p \text{ points to value } \nu \\
& \quad | S, p: e \ @ M & \quad p \text{ points to thunk } e, \text{ run in scope } M
\end{align*}
\]

\textbf{Notation:} \(S[p\rightarrow \nu]\) and \(S[p\rightarrow e@M]\) extend \(S\) at \(p\) when \(p \not\in \text{dom}(S)\). \(S[p\rightarrow e@M]\) overwrite \(S\) at \(p\) when \(p \in \text{dom}(S)\).

\[\frac{\nu \downarrow S_2; t}{S_1 \vdash^M_m e \downarrow S_2; t}\] Under store \(S\) in namespace \(M\) at current node \(m\), expression \(e\) produces new store \(S_2\) and result \(t\).

\[\frac{S_1 \vdash^M_m (v_2/x_2)[v_1/x_1]e \downarrow S_2; e'}{S_1 \vdash^M_m \text{split}((v_1, v_2), x_1.x_2.e) \downarrow S_2; e'}\] \(\Downarrow\)-split

\[\frac{S_1 \vdash^M_m [v/x]e \downarrow S_2; e'}{S_1 \vdash^M_m \text{vunpack}(\text{pack}(a.v), b.x.e) \downarrow S_2; e'}\] \(\Downarrow\)-unpack

\[\frac{S_1 \vdash^M_m e_1 \downarrow S_1'; \text{ret}(v)}{S_1' \vdash^M_m [v/x]e_2 \downarrow S_2'; e_2'}\] \(\Downarrow\)-let

\[\frac{S_1 \vdash^M_m \text{let}(e_1, x.e_2) \downarrow S_2'; e_2'}{S_1 \vdash^M_m e_1 \downarrow S_1'; \lambda x. e_2}\] \(\Downarrow\)-app

\[\frac{S_1 \vdash^M_1 \circ^M_2 e \downarrow S_2'; e'}{S_1 \vdash^M_1 \text{scope}(M_2, e) \downarrow S_2'; e'}\] \(\Downarrow\)-scope

\[\frac{M_1 \downarrow^M \lambda \alpha. M_2}{S \vdash^M M_1 (\text{name } n) \downarrow S; \text{ret(name } n)}\] \(\Downarrow\)-name-app

\[\frac{(M.n) \downarrow^M p}{S_1 \vdash^M \text{thunk}(\text{name } n, e) \downarrow S_2; \text{ret(thunk } p)}\] \(\Downarrow\)-thunk

\[\frac{(M.n) \downarrow^M p}{S \vdash^M \text{ref(name } n, v) \downarrow S_2; \text{ret(ref } p)}\] \(\Downarrow\)-ref

\[\frac{S(p) = e \ @ M_0}{S \vdash^M \text{force(thunk } p) \downarrow S_2; t}\] \(\Downarrow\)-force

\[\frac{S(p) = v}{S \vdash^M \text{get(ref } p) \downarrow S; \text{ret(} v)}\] \(\Downarrow\)-get

\[\frac{S \vdash^M t}{S \vdash^M t \downarrow S; t}\] \(\Downarrow\)-term

Fig. 19. Dynamic semantics, complete
\[ \mathcal{D} \text{ by } \Downarrow\text{-term}() \text{ reads } \emptyset \text{ writes } \emptyset \]

\[ \mathcal{D} \text{ by } \Downarrow\text{-app}(\mathcal{D}_1, \mathcal{D}_2) \text{ reads } R_1 \cup (R_2 - W_1) \text{ writes } W_1 \perp W_2 \quad \text{if} \quad \mathcal{D}_1 \text{ reads } R_1 \text{ writes } W_1 \]

\[ \text{ and } \mathcal{D}_2 \text{ reads } R_2 \text{ writes } W_2 \]

\[ \mathcal{D} \text{ by } \Downarrow\text{-let}(\mathcal{D}_1, \mathcal{D}_2) \text{ reads } R_1 \cup (R_2 - W_1) \text{ writes } W_1 \perp W_2 \quad \text{if} \quad \mathcal{D}_1 \text{ reads } R_1 \text{ writes } W_1 \]

\[ \text{ and } \mathcal{D}_2 \text{ reads } R_2 \text{ writes } W_2 \]

\[ \mathcal{D} \text{ by } \Downarrow\text{-scope}(\mathcal{D}_0) \text{ reads } R \text{ writes } W \quad \text{if} \quad \mathcal{D}_0 \text{ reads } R \text{ writes } W \]

\[ \mathcal{D} \text{ by } \Downarrow\text{-case}(\mathcal{D}_0) \text{ reads } R \text{ writes } W \quad \text{if} \quad \mathcal{D}_0 \text{ reads } R \text{ writes } W \]

\[ \mathcal{D} \text{ by } \Downarrow\text{-split}(\mathcal{D}_0) \text{ reads } R \text{ writes } W \quad \text{if} \quad \mathcal{D}_0 \text{ reads } R \text{ writes } W \]

\[ \mathcal{D} \text{ by } \Downarrow\text{-ref}() \text{ reads } \emptyset \text{ writes } p \quad \text{where } e = \text{ref(name } n, v) \text{ and } p \equiv M n \]

\[ \mathcal{D} \text{ by } \Downarrow\text{-thunk}() \text{ reads } \emptyset \text{ writes } p \quad \text{where } e = \text{thunk(name } n, e_0) \text{ and } p \equiv M n \]

\[ \mathcal{D} \text{ by } \Downarrow\text{-get}() \text{ reads } p \text{ writes } \emptyset \quad \text{where } e = \text{get(ref } p) \]

\[ \mathcal{D} \text{ by } \Downarrow\text{-force}() \text{ reads } q, R' \text{ writes } W' \quad \text{where } e = \text{force(thunk } q) \]

\[ \text{ and } \quad \mathcal{D}' \text{ reads } R' \text{ writes } W' \quad \text{where } \mathcal{D}' \text{ is the derivation that computed } t \]

Fig. 20. Read- and write-sets of a non-incremental evaluation derivation
Under $\Gamma$, value type $A$ has kind $K$.

\begin{align*}
\Gamma \vdash A : K \\
(\alpha : K) \in \Gamma \\
\frac{\Gamma \vdash \alpha : K}{\Gamma \vdash \alpha : K} & \quad \text{k-typevar} \\
(d : K) \in \Gamma \\
\frac{\Gamma \vdash d : K}{\Gamma \vdash d : K} & \quad \text{k-tycon} \\
\Gamma \vdash A_1 : \text{type} & \quad \Gamma \vdash A_2 : \text{type} \\
\frac{\Gamma \vdash (A_1 + A_2) : \text{type}}{\text{k-binop}} \\
\Gamma \vdash (A_1 \times A_2) : \text{type} \\
\Gamma \vdash \text{unit} : \text{type} & \quad \text{k-unit} \\
\Gamma \vdash \text{NmSet} & \quad \text{k-name} \\
\frac{\Gamma \vdash \text{Nm}[i] : \text{type}}{\Gamma \vdash \text{Nm}[i] : \text{type}} \\
\Gamma \vdash E : \text{efftype} & \quad \text{k-thk} \\
\frac{\Gamma \vdash (\text{Thk}[i] E) : \text{type}}{\Gamma \vdash (\text{Thk}[i] E) : \text{type}} \\
\Gamma, \alpha : \gamma \vdash P : \text{prop} & \quad \Gamma, \alpha : \gamma \vdash A : \text{type} \\
\frac{\Gamma \vdash (\forall \alpha : \gamma. P. A) : \text{type}}{\Gamma \vdash (\forall \alpha : \gamma. P. A) : \text{type}} & \quad \text{k-all} \\
\Gamma, a : \gamma \vdash P : \text{prop} & \quad \Gamma, a : \gamma \vdash A : \text{type} \\
\frac{\Gamma \vdash (\forall a : \gamma. P. A) : \text{type}}{\Gamma \vdash (\forall a : \gamma. P. A) : \text{type}} & \quad \text{k-exists} \\
\Gamma \vdash C : \text{ctype} & \quad \text{Under } \Gamma, \text{ computation type } C \text{ is well-formed} \\
\frac{\Gamma \vdash A : \text{type}}{\Gamma \vdash (\text{F} A) : \text{ctype}} & \quad \text{ctype-lift} \\
\frac{\Gamma \vdash E \text{ efftype}}{\Gamma \vdash (A \rightarrow E) \text{ efftype}} & \quad \text{ctype-arr} \\
\Gamma \vdash \epsilon : \text{wf-effects} & \quad \text{Under } \Gamma, \text{ effects } \epsilon \text{ are well-formed} \\
\frac{\Gamma \vdash W : \text{NmSet}}{\Gamma \vdash W; R : \text{NmSet}} & \quad \text{wf-eff} \\
\Gamma \vdash \text{Prop} & \quad \text{Under } \Gamma, \text{ proposition } \text{Prop} \text{ is well-formed} \\
\frac{\Gamma \vdash P_1 \text{ prop}}{\Gamma \vdash (P_1 \text{ and } P_2) \text{ prop}} & \quad \text{prop} \\
\frac{\Gamma \vdash i : \gamma}{\Gamma, a : \gamma \vdash P \text{ prop}} & \quad \Gamma, a : \gamma \vdash A : \text{type} \\
\frac{\Gamma \vdash (\exists a : \gamma. P. A) : \text{type}}{\Gamma \vdash (\exists a : \gamma. P. A) : \text{type}} & \quad \text{k-exists} \\
\frac{\Gamma \vdash C : \text{ctype} \quad \Gamma \vdash \epsilon : \text{wf-effects}}{\Gamma \vdash (C \triangleright \epsilon) \text{ efftype}} & \quad \text{etyp-arr} \\
\frac{\Gamma, \alpha : K \vdash E \text{ efftype}}{\Gamma \vdash (\forall \alpha : K. E) \text{ efftype}} & \quad \text{etyp-poly} \\
\frac{\Gamma, a : \gamma \vdash P \text{ prop}}{\Gamma \vdash (\forall a : \gamma. P. E) \text{ efftype}} & \quad \text{etyp-idx} \\
\end{align*}

Fig. 21. Kinding and well-formedness for types and effects.
A.3 Remarks

Why distinguish computation types from types-with-effects? Can we unify computation types C and types-with-effects E? Not easily. We have two computation types, F and →. For F, the expression being typed could create a thunk, so we must put that effect somewhere in the syntax. For →, applying a function is (per call-by-push-value) just a “push”: the function carries no effects of its own (though its codomain may need to have some). However, suppose we force a thunked function of type \(A_1 \rightarrow (A_2 \rightarrow \cdots)\) and apply the function (the contents of the thunk) to one argument. In the absence of effects, the result would be a computation of type \(A_2 \rightarrow \cdots\), meaning that the computation is waiting for a second argument to be pushed. But, since forcing the thunk has the effect of reading the thunk, we need to track this effect in the result type. So we cannot return \(A_2 \rightarrow \cdots\), and must instead put effects around \((A_2 \rightarrow \cdots)\). Thus, we need to associate effects to both F and →, that is, to both computation types.

Now we are faced with a choice: we could (1) extend the syntax of each connective with an effect (written next to the connective), or (2) introduce a “wrapper” that encloses a computation type, either F or →. These seem more or less equally complicated for the present system, but if we enriched the language with more connectives, choice (1) would make the new connectives more complicated, while under choice (2), the complication would already be rolled into the wrapper. We choose (2), and write the wrapper as \(C \triangleright e\), where C is a computation type and e represents effects.

Where should these wrappers live? We could add \(C \triangleright e\) to the grammar of computation types C. But it seems useful to have a clear notion of the effect associated with a type. When the effect on the outside of a type is the only effect in the type, as in \((A_1 \rightarrow F A_2) \triangleright e\), “the” effect has to be e. Alas, types like \((C \triangleright e_1) \triangleright e_2\) raise awkward questions: does this type mean the computation does \(e_2\) and then \(e_1\), or \(e_1\) and then \(e_2\)?

We obtain an unambiguous, singular outer effect by distinguishing types-with-effects E from computation types C. The meta-variables for computation types appear only in the production \(E := C \triangleright e\), making types-with-effects E the “common case” in the grammar. Many of the typing rules follow this pattern, achieving some isolation of effect tracking in the rules.

Future work: Editor and Archivist. To distinguish imperative name allocation from name-precise computation, future versions of Fungi will introduce two incremental computation roles, which we term the editor and the archivist, respectively; specifically, we define the syntax for roles as \(\tau := ed \mid ar\). The archivist role (ar) corresponds to computation whose dependencies we cache, and the editor role (ed) corresponds to computation that feeds the archivist with input changes, and demands any changed output that is relevant; in short, the editor represents the world outside the cached computation.

While the current type system prototype focuses only on the archivist role, leaving the editor role to the surrounding Rust code, future work will integrate the editor role into Fungi programs. For example, consider the following typing rules, which approximate (and extend) our full type system with a role \(\tau\) in each rule:

\[
\begin{align*}
\Gamma, v_n : \text{Nm}[X] & \quad \Gamma, v : A \\
\Gamma \vdash e_1 : A \triangleright ar(X) & \quad \Gamma, x : A \vdash e_2 : B \triangleright ar(Y) \\
\Gamma \vdash (X \triangleleft Y) \equiv Z : \text{NmSet} & \quad \Gamma \vdash (X \triangleleft Y) \equiv Z : \text{NmSet} \\
\Gamma, v_n, v : \text{Ref}[A] \triangleright \tau(X) & \quad \Gamma \vdash \text{let}(e_1, x, e_2) : B \triangleright ar(Z) \\
\Gamma \vdash \text{let}(e_1, x, e_2) : B \triangleright ed(Z) & \quad \Gamma \vdash \text{let}(e_1, x, e_2) : B \triangleright ed(Z)
\end{align*}
\]

These rules are similar to the simplified rules presented in Sec. 2. In contrast to those rules, these conclude with the judgement form \(\Gamma \vdash e : A \triangleright \tau(X)\), mentioning the written set with the notation \(\triangleright \tau(X)\), where the set X approximates the set of written names (as in the earlier formulation), and \(\tau\) is the role (absent from the earlier formulation).

Matthew A. Hammer, Jana Dunfield, Kyle Headley, Monal Narasimhamurthy, and Dimitrios J. Economou
The first rule types a reference cell allocation, as before; in the rule’s conclusion, this name set \( X \) serves as the allocation’s write set. The undetermined role \( r \) means that this rule is applicable to both the editor and the archivist roles.

What was one let sequencing rule (in Sec. 2) is now two rules here: The second rule enforces the archivist role, where names are precise. The third rule permits the editor role, where names allocated later may overwrite names allocated earlier. Finally, a new syntax form \( \text{archivist}(e) \) permits the editor’s computations to delegate to archivist sub-computations; the program \( \text{archivist}(e) \) has role \( r \) whenever program \( e \) types under role \( r \) under the same typing context.

Among the future work for mixing these roles, we foresee that extending the theory of Fungi, including covariant index subtyping, to this mixture of imperative-functional execution semantics requires mixing imperative effects (for the editor) and type index subtyping (for the archivist) in a disciplined, sound manner.

B OMITTED LEMMAS AND PROOFS

**Lemma B.1 (Index-level weakening).**

1. If \( \Gamma \vdash M : \gamma \) then \( \Gamma, \Gamma' \vdash M : \gamma \).
2. If \( \Gamma \vdash i : \gamma \) then \( \Gamma, \Gamma' \vdash i : \gamma \).
3. If \( \Gamma \vdash A : K \) then \( \Gamma, \Gamma' \vdash A : K \).

**Proof.** By induction on the given derivation. \( \square \)

**Lemma B.2 (Weakening).**

1. If \( \Gamma \vdash e : A \) then \( \Gamma, \Gamma' \vdash e : A \).
2. If \( \Gamma \vdash M e : C \) then \( \Gamma, \Gamma' \vdash M e : C \).

**Proof.** By induction on the given derivation, using Lemma F.1 (Weakening of semantic equivalence and apartness) (for example, in the case for the value typing rule ‘name’) and Lemma B.1 (Index-level weakening) (for example, in the case for the computation typing rule ‘AllIndexElim’). \( \square \)

**Lemma B.3 (Substitution).**

1. If \( \Gamma \vdash v : A \) and \( \Gamma, x : A \vdash e : C \) then \( \Gamma \vdash [v/x]e : C \).
2. If \( \Gamma \vdash v : A \) and \( \Gamma, x : A \vdash v' : B \) then \( \Gamma \vdash [v/x]v' : B \).

**Proof.** By mutual induction on the derivation typing \( e \) (in part 1) or \( v' \) (in part 2). \( \square \)

In the presence of subtyping, canonical forms (value inversion) is not entirely straightforward.

**Lemma B.4 (Subtyping Weakening).** If \( \Gamma \vdash A \leq V B \) then \( \Gamma, \Gamma' \vdash A \leq V B \) where \( \Gamma' \) consists of \( a : \gamma \) and \( P \) assumptions.

**Proof.** By induction on the derivation of \( \Gamma \vdash A \leq V B \). In the \( \leq V \)-name, \( \leq V \)-namefn, \( \leq V \)-ref, \( \leq V \)-thk, \( \leq V \)-VL and \( \leq V \)-\( \exists \) cases, use weakening for the relations \( \vdash \) and \( \models \). \( \square \)

**Lemma B.5 (Subtyping Substitution).**

If \( \Gamma, \alpha : \gamma, P \vdash A \leq V B \) and \( \Gamma \vdash i : \gamma \) and \( \text{extract}(\Gamma) \models P \) then \( \Gamma \vdash [i/\alpha]A \leq V [i/\alpha]B \).

**Proof.** By induction on the derivation of \( \Gamma \vdash A \leq V B \). In the \( \leq V \)-ref, \( \leq V \)-thk, \( \leq V \)-VL and \( \leq V \)-\( \exists \) cases, use substitution for the relation \( \models \). \( \square \)

**Lemma B.6 (Reflexivity of Subtyping).** For all \( \Gamma \) and \( A \), it is the case that \( \Gamma \vdash A \leq V A \).

**Proof.** Immediate by rule \( \leq V \)-refl. \( \square \)
Lemma B.7 (Transitivity of Subtyping).
If $\Gamma \vdash A_L \leq V B$ and $\Gamma \vdash B \leq V A_R$ then $\Gamma \vdash A_L \leq V A_R$.

Proof. By simultaneous induction on the two given derivations. If either derivation is by $\leq V\text{-refl}$, we already have our result. Consider cases of the rule concluding $\Gamma \vdash A_L \leq V B$.

- $\leq V\times$:
The derivation of $\Gamma \vdash B \leq V A_R$ must be by $\leq V\text{-refl}$ (already handled), $\leq V\times$ or $\leq V\forall R$.
  If by $\leq V\times$, the result follows by using the i.h. twice on the respective subderivations, then applying $\leq V\times$.
  If by $\leq V\forall R$, then:
  \[
  A_R = (\forall b : \gamma \mid P. A_{R0})
  \]
  By inversion ($\leq V\forall R$)
  $\Gamma, b : \gamma, P \vdash B \leq V A_{R0}$
  Given
  $\Gamma, b : \gamma, P \vdash A_L \leq V B$
  By Lemma B.4 (Subtyping Weakening)
  $\Gamma, b : \gamma, P \vdash A_L \leq V A_{R0}$
  By i.h.
  $\Gamma \vdash A_L \leq V (\forall b : \gamma \mid P. A_{R0})$
  By $\leq V\forall R$
  $\Gamma \vdash A_L \leq V A_R$
  By above equation

- $\leq V\vdash$: Similar to the $\leq V\times$ case.

- $\leq V\text{name}$, $\leq V\text{ref}$, $\leq V\text{thk}$: Similar to the $\leq V\times$ case, using transitivity of $\subseteq$ at the index level.

- $\leq V\text{namefn}$: Use transitivity of $\text{conv}$.

- $\leq V\forall L$:
  By i.h., $\Gamma \vdash [i/a]A_{L0} \leq V A_R$.
  By $\leq V\forall L$, $\Gamma \vdash \forall a : \gamma \mid P. A_{L0} \leq V A_R$, which was to be shown.

- $\leq V\forall R$:
The other derivation is by either $\leq V\text{-refl}$ (already handled) or $\leq V\forall L$.

  \[
  B = (\forall b : \gamma \mid P. B_0)
  \]
  By inversion ($\leq V\forall R$)
  $\Gamma, b : \gamma, P \vdash A_L \leq V B_0$
  By inversion ($\leq V\forall L$)
  $\Gamma \vdash i : \gamma$
  By Lemma B.5 (Subtyping Substitution)
  $\Gamma \vdash [i/b]0 \leq V A_R$
  By i.h.
  $\Gamma \vdash [i/b]A_L \leq V [i/b]B_0$
  $\Gamma \vdash [i/b]A_L \leq V A_R$
  By above equation

\[\square\]
**LEMMA B.8 (CANONICAL FORMS).** Suppose \( \Gamma \) store-type and \( \Gamma \vdash \nu : \mathcal{A} \).

1. If \( \mathcal{A} \leq \nu \) unit
   
   then \( \nu = () \).

2. If \( \mathcal{A} \leq \nu (\mathcal{B}_1 \times \mathcal{B}_2) \)
   
   then \( \nu = (\nu_1, \nu_2) \) and \( \Gamma \vdash \nu_1 : \mathcal{B}_1 \) and \( \Gamma \vdash \nu_2 : \mathcal{B}_2 \).

3. If \( \mathcal{A} \leq \nu (\mathcal{B}_1 + \mathcal{B}_2) \)
   
   then \( \nu = \text{inj}_i \nu_i \) where \( i \in \{1, 2\} \) and \( \Gamma \vdash \nu_i : \mathcal{B}_i \).

4. If \( \mathcal{A} \leq \nu (\text{Name}[\mathcal{X}]) \)
   
   then \( \nu = \text{name } \pi \) where \( \Gamma \vdash \pi \in \mathcal{X} \).

5. If \( \mathcal{A} \leq \nu (\text{Ref}[\mathcal{X}] \mathcal{A}_0) \)
   
   then \( \nu = \text{ref } \pi \) where \( \Gamma \vdash \pi \in \mathcal{X} \).

6. If \( \mathcal{A} \leq \nu (\text{Thk}[\mathcal{X}] \mathcal{E}) \)
   
   then \( \nu = \text{thunk } \pi \) where \( \Gamma \vdash \pi \in \mathcal{X} \).

7. If \( \mathcal{A} \leq \nu (\text{Nm} \overset{\rightarrow}{\Rightarrow} \text{Nm})[\mathcal{M}] \)
   
   then \( \nu = \text{nmfn } \mathcal{M}_\nu \) where \( \mathcal{M} =_\beta (\lambda \alpha. \mathcal{M}^') \) and \( \vdash (\lambda \alpha. \mathcal{M}^') : (\text{Nm} \overset{\rightarrow}{\Rightarrow} \text{Nm}) \) and \( \mathcal{M}_\nu =_\beta \mathcal{M} \).

**PROOF.** By induction on the derivation of \( \Gamma \vdash \mathcal{A} \leq \nu \) \( \mathcal{B} \).

(1) Consider cases of the rule concluding \( \Gamma \vdash \nu : \mathcal{A} \).

- **Case unit:** By inversion.

- **Case pair:** Impossible because \( \Gamma \vdash \mathcal{A}_1 + \mathcal{A}_2 \leq \nu \) unit is not derivable.

- **Case name:** Impossible because \( \Gamma \vdash \text{Name}[\mathcal{X}] \leq \nu \) unit is not derivable.

- **Case namefn:** Impossible because \( \Gamma \vdash (\text{Name} \overset{\rightarrow}{\Rightarrow} \text{Name})[\mathcal{M}] \leq \nu \) unit is not derivable.

- **Case ref:** Impossible because \( \Gamma \vdash (\text{Ref}[\mathcal{X}] \mathcal{A}_0) \leq \nu \) unit is not derivable.

- **Case thunk:** Impossible because \( \Gamma \vdash (\text{Thk}[\mathcal{X}] \mathcal{E}) \leq \nu \) unit is not derivable.

- **Case vtype-\( \forall \)IndexIntro:**

\[
\Gamma \vdash (\forall a : \gamma | \mathcal{P} \mathcal{A}_0) \leq \nu \text{ unit}
\]

Given

\[
\begin{align*}
\Gamma, a : \gamma, \mathcal{P} &\vdash \mathcal{A}_0 \leq \nu \text{ unit} & \text{By inversion (\( \leq \nu - \forall \))} \\
\Gamma, a : \gamma, \mathcal{P} &\vdash \nu : \mathcal{A}_0 & \text{Subderivation} \\
\Gamma, a : \gamma, \mathcal{P} &\vdash \nu = () & \text{By i.h. (part 1)}
\end{align*}
\]

- **Case vtype-\( \exists \)IndexIntro:**

Impossible because \( \Gamma \vdash (\exists a : \gamma | \mathcal{P} \mathcal{A}_0) \leq \nu \) unit is not derivable.

(2) \( \times \):

Consider cases of the rule concluding \( \Gamma \vdash \nu : \mathcal{A} \).

- **Case unit:** Impossible because \( \Gamma \vdash \text{unit} \leq \nu (\mathcal{B}_1 \times \mathcal{B}_2) \) is not derivable.

- **Case pair:**
Given \( \Gamma \vdash A \leq V (B_1 \times B_2) \),
\[ A = (A_1 \times A_2) \]
By inversion (pair)
\[ v = (v_1, v_2) \]
\[ \Gamma \vdash v_1 : B_1 \]
\[ \Gamma \vdash v_2 : B_2 \]
\[ \Gamma \vdash A_1 \leq V B_1 \]
By inversion (\( \preceq V \times \))
\[ \Gamma \vdash A_2 \leq V B_2 \]
By \( \preceq V \times \)-vtype-sub
\[ Z \Gamma \vdash v_1 : B_1 \]
\[ Z \Gamma \vdash v_2 : B_2 \]

- Cases name, namefn, ref, thunk:
  Impossible because the assumed subtyping is not derivable.

- Case vtype-\( \forall \)IndexIntro:
  \[ \Gamma \vdash (\forall a : \gamma \mid P. A_0) \leq V (B_1 \times B_2) \]
  Given
  \[ \Gamma, a : \gamma, P \vdash A_0 \leq V (B_1 \times B_2) \]
  By inversion (\( \leq V \forall \))
  \[ \Gamma, a : \gamma, P \vdash v : A_0 \]
  Subderivation
  \[ \Gamma \vdash v_1 : B_1 \]
  By i.h. (part 2)
  \[ \Gamma \vdash v_2 : B_2 \]
  By i.h. (part 2)

- Case extract(\( \Gamma \)) \( \vdash [i/a]P \)
  \[ \Gamma \vdash i : \gamma \]
  Subderivation
  \[ \Gamma \vdash v : (\forall a : \gamma \mid P. A_0) \]
  vtype-\( \forall \)IndexElim
  \[ \Gamma \vdash [i/a]A_0 \leq V A \]
  Given
  \[ \Gamma \vdash (\forall a : \gamma \mid P. A_0) \leq V ([i/a]A_0) \]
  By \( \leq V \forall \)
  \[ \Gamma \vdash [i/a]A_0 \leq V A \]
  By Lemma B.7 (Transitivity of Subtyping)
  \[ \Gamma \vdash v : (\forall a : \gamma \mid P. A_0) \]
  Subderivation
  \[ \Gamma \vdash v = (v_1, v_2) \]
  By i.h. (part 2)
  \[ \Gamma \vdash v_1 : B_1 \]
  By i.h. (part 2)
  \[ \Gamma \vdash v_2 : B_2 \]
  By i.h. (part 2)

- Case vtype-\( \exists \)IndexIntro:
  Impossible because \( \Gamma \vdash (\exists a : \gamma \mid P. A_0) \leq V (B_1 \times B_2) \) is not derivable.

(3) +: Similar to Part 2.
(4) \( \text{Nm}[X] \):
  In the \( \leq V \)-name case, use the fact that \( \Gamma \vdash X' \subseteq X \) and \( \Gamma \vdash n \in X \) implies \( \Gamma \vdash n \in X \).
  Otherwise similar to Part 1.
(5) \( \text{Ref}[X] A_0 \): Similar to Parts 1 and 4.
(6) \( \text{Thk}[X] E \): Similar to Part 5.
(7) \( (\text{Nm} \Rightarrow \text{Nm})[M] \): Similar to Part 5.

\( \square \)
LEMMA B.9 (APPLICATION AND MEMBERSHIP Commute). If \( \Gamma \vdash n \in i \) and \( p \in M(i) \) then \( \Gamma \vdash p \in M(i) \).

Proof. The set \( M(i) \) consists of all elements of \( i \), but mapped by function \( M \). The name \( p \) is convertible to the name \( M(n) \). Since \( n \in i \), we have that \( p \) is in the \( M \)-mapping of \( i \), which is \( M(i) \). \( \square \)

In each case, we write “\( \Rightarrow \)” to the left of each goal, as we prove it.

THEOREM 6.1 (SUBJECT REDUCTION). If \( \Gamma_1 \) store-type and \( \Gamma_1 \vdash M : \text{Nm} \Rightarrow X \text{Nm} \) and \( \Gamma_1 \vdash M : e : C \rhd (W; R) \) and \( \vdash S_1 : \Gamma_1 \) and \( D \) derives \( S_1 \vdash M \). \( e \) \( \vdash S_2 : \Gamma_2 \) and \( \vdash t : C \rhd (\emptyset; \emptyset) \) and \( D \) reads \( R_D \) writes \( W_D \) and \( \langle W_D; R_D \rangle \leq \langle W; R \rangle \).

Proof. By induction on the derivation \( S \) of \( \Gamma_1 \vdash M : e : C \rhd (W; R) \).

- **Case** \( \Gamma_1 \vdash v : A \)

  \[
  \begin{array}{c}
  \Gamma_1 \vdash v : A \\
  \hline
  (e = t) \text{ and } (S_1 = S_2) \text{ Given} \\
  (R_D = W_D = R = W = \emptyset) \text{ "} \\
  (\Gamma_2 = \Gamma_1) \text{ Suppose} \\
  \vdash S_2 : \Gamma_2 \text{ by above equalities} \\
  \vdash t : C \rhd (\emptyset; \emptyset) \text{ "} \\
  \langle W_D; R_D \rangle \leq \langle W; R \rangle \text{ All are empty}
  \end{array}
  \]

- **Case** \( \Gamma_1 \vdash v : \text{Ref[X]} A \)

  \[
  \begin{array}{c}
  \Gamma_1 \vdash v : \text{Ref[X]} A \\
  \hline
  (W = \emptyset) \text{ and } (R = X) \text{ Given} \\
  \exists p. \ (v = \text{ref } p) \text{ Lemma B.8 (Canonical Forms)} \\
  \Gamma_1 \vdash p \in X \text{ "} \\
  \Gamma_1(p) = A \text{ By inversion of value typing} \\
  \exists \nu_p. \ S_1(p) = \nu_p \text{ Inversion on } \vdash S_1 : \Gamma_1 \\
  \Gamma_1 \vdash \nu_p : A \text{ "} \\
  (\Gamma_2 = \Gamma_1) \text{ and } (t = \text{ret}(\nu_p)) \text{ Suppose} \\
  (R_D = [p]) \text{ and } (W_D = W = \emptyset) \text{ "} \\
  \vdash S_2 : \Gamma_2 \text{ by above equalities} \\
  \vdash t : C \rhd (\emptyset; \emptyset) \text{ "} \\
  \langle W_D; R_D \rangle \leq \langle W; R \rangle \text{ By above equality } W_D = W = \emptyset, \\
  \ldots \text{ and inequality for } (R_D = [p]) \subseteq (X = R).
  \end{array}
  \]

- **Case** \( \Gamma_1 \vdash v : \text{Thk[X]} (C \rhd \epsilon) \)

  \[
  \begin{array}{c}
  \Gamma_1 \vdash v : \text{Thk[X]} (C \rhd \epsilon) \\
  \hline
  \text{force}(v) : (C \rhd (\emptyset; X) \text{ and } \epsilon)
  \end{array}
  \]
\[ \Gamma \vdash e : \tau \quad \text{Given} \]
\[ \Gamma \vdash e : \tau \quad \text{Given} \]
\[ (W = \emptyset) \text{ and } (R = X) \quad \text{Given} \]
\[ \Gamma_1 \vdash \nu : \text{Thk}[X] \quad (C \triangleright e) \quad \text{Given} \]
\[ \exists p. \, (\nu = \text{thunk } p) \quad \text{Lemma B.8 (Canonical Forms)} \]
\[ \Gamma_1 \vdash p \in X \quad \text{"} \]
\[ \Gamma_1 (p) = (C \triangleright e) \quad \text{By inversion of value typing} \]
\[ \exists e_p. \, S_1 (p) = e_p \quad \text{Inversion on } \vdash S_1 : \Gamma_1 \]
\[ S_0 :: \quad \Gamma_1 \vdash e_p : (C \triangleright e) \quad \text{"} \]
\[ D_0 :: \quad S_1 \vdash^M_{\text{m}} e_p \Downarrow S_2 ; t \quad \text{Inversion of } D \]
\[ \vdash S_2 : \Gamma_2 \quad \text{By i.h. on } S_0 \text{ and } D_0 \]
\[ \vdash \Gamma_2 + t : C \triangleright (\emptyset, \emptyset) \quad \text{"} \]
\[ D_0 \text{ reads } R_{D_0} \text{ writes } W_{D_0} \quad \text{"} \]
\[ \langle W_{D_0} ; R_{D_0} \rangle \leq \langle W ; R \rangle \quad \text{"} \]
\[ D \text{ reads } R_{D_0} \text{ writes } W_{D_0} \quad \text{By Def. 6.2} \]
\[ \langle W_{D_0} ; R_{D_0} \rangle \leq \langle W ; R \rangle \quad \text{by above equality } W_{D_0} = W = \emptyset, \]
\[ \ldots \text{ and inequality } (R_{D} = \{p\}) \subseteq (X = R). \]

### Case

\[ \Gamma_1 \vdash \nu : (\text{Nm} \text{Nm})[M'] \quad \Gamma_1 \vdash^M_{\text{P}} e_0 : C \triangleright \langle W ; R \rangle \]

\[ S_0 :: \quad \Gamma_1 \vdash^M_{\text{P}} e_0 : C \triangleright \langle W ; R \rangle \quad \text{Subderivation 2 of } S \]
\[ D :: \quad S_1 \vdash^M_{\text{m}} \text{scope}(\nu, e_0) \Downarrow S_2 ; t \quad \text{Given} \]
\[ D_0 :: \quad S_1 \vdash^M_{\text{m}} \text{scope}(\nu, e_0) \Downarrow S_2 ; t \quad \text{By inversion (scope)} \]

\[ \Gamma_1 \vdash M : \text{Nm} \text{Nm} \quad \text{Assumption} \]
\[ \Gamma_1 \vdash \nu : (\text{Nm} \text{Nm})[M'] \quad \text{Subderivation 1 of } S \]
\[ \Gamma_1 \vdash M' : \text{Nm} \text{Nm} \quad \text{By inversion} \]
\[ \Gamma_1, x : \text{Nm} \vdash M' : \text{Nm} \quad \text{By rule t-app} \]
\[ \Gamma_1, x : \text{Nm} \vdash M (M' x) : \text{Nm} \quad \text{By rule t-app} \]
\[ \Gamma_1 \vdash \lambda x. M (M' x) : \text{Nm} \quad \text{By rule t-abs} \]
\[ \Gamma_1 \vdash (M o M') : \text{Nm} \quad \text{By definition of } M o M' \]

\[ \vdash S_2 : \Gamma_2 \quad \text{By i.h. on } S_0 \]
\[ \vdash \Gamma_2 + t : C \triangleright (\emptyset, \emptyset) \quad \text{"} \]
\[ D_0 \text{ reads } R_{D_0} \text{ writes } W_{D_0} \quad \text{"} \]
\[ \langle W_{D_0} ; R_{D_0} \rangle \leq \langle W ; R \rangle \quad \text{"} \]
\[ D \text{ reads } R_{D} \text{ writes } W_{D} \quad \text{By Def. 6.2} \]
\[ \langle W_{D} ; R_{D} \rangle = \langle W_{D_0} ; R_{D_0} \rangle \quad \text{"} \]
\[ \langle W_{D} ; R_{D} \rangle \leq \langle W ; R \rangle \quad \text{By above equalities} \]

### Case

\[ \Gamma_1 \vdash \nu : \text{Nm}[X] \quad \Gamma_1 \vdash e : E \quad \text{thunk} \]
\[ \Gamma_1 \vdash^M \text{thunk}(\nu_1, \nu_2) : F (\text{Thk}[M(X)] E) \triangleright \langle M(X); \emptyset \rangle \]
\[ C = F (\text{Thk}[M(X)] E) \text{ and } R = \emptyset \text{ and } W = M(X) \quad \text{Given from } S \]
\[ \Gamma_1 \vdash v : Nm[X] \quad \text{Subderivation} \]
\[ (v = \text{name } n) \text{ and } (n \in X) \quad \text{By Lemma B.8} \]
\[ M \downarrow p \text{ and } R_D = \emptyset \text{ and } W_D = \{p\} \quad \text{Given from } D \]
\[ S_2 = (S_1, p : e) \quad " \]
\[ \Gamma_2 = (\Gamma_1, p : \text{Thk}[p] E) \quad \text{Suppose} \]
\[ \vdash S_2 : \Gamma_2 \quad \text{By rule (Fig. 18)} \]
\[ \Gamma_2(p) = E \quad \text{By inversion of value typing} \]
\[ \Gamma_2 \vdash \text{ref } p : \text{Ref}[p] E \quad \text{By rule thunk} \]
\[ \Gamma_2 \vdash^M \text{ret}(\text{thunk } p) : F (\text{Ref}[M(X)] A) \triangleright \langle \emptyset; 0 \rangle \quad \text{By rule ret} \]
\[ D \text{ reads } R_D \text{ writes } W_D \text{ and } W_D = \{p\} \quad \text{By Def. 6.2} \]
\[ n \in X \quad \text{Above} \]
\[ M(n) \in M(X) \quad \text{Name term application is pointwise} \]
\[ M(n) \in W \quad \text{By above equality} \]
\[ M(n) = p \]
\[ \{p\} \subseteq W \quad \text{By set theory} \]
\[ \langle W_D; R_D \rangle \leq \langle W; R \rangle \]

- **Case**

\[ \Gamma_1 \vdash v_1 : Nm[X] \quad \Gamma_1 \vdash v_2 : A \]
\[ \Gamma_1 \vdash^M \text{ref}(v_1, v_2) : F (\text{Ref}[M(X)] A) \triangleright \langle M(X); 0 \rangle \]
\[ C = F (\text{Ref}[M(X)] A) \text{ and } R = \emptyset \text{ and } W = M(X) \quad \text{Given from } S \]
\[ \Gamma_1 \vdash v_1 : Nm[X] \quad \text{Subderivation} \]
\[ (v_1 = \text{name } n) \text{ and } (n \in X) \quad \text{Lemma B.8 (Canonical Forms)} \]
\[ M \downarrow p \text{ and } R_D = \emptyset \text{ and } W_D = \{p\} \quad \text{Given from } D \]
\[ S_2 = (S_1, p : v_2) \quad " \]
\[ \Gamma_2 = (\Gamma_1, p : \text{Ref}[p] A) \quad \text{Suppose} \]
\[ \vdash S_2 : \Gamma_2 \quad \text{By rule (Fig. 18)} \]
\[ \Gamma_2(p) = A \quad \text{By inversion of value typing} \]
\[ \Gamma_2 \vdash \text{ref } p : \text{Ref}[p] A \quad \text{By rule ref} \]
\[ \Gamma_2 \vdash^M \text{ret}(\text{ref } p) : \text{ret}(\text{Ref}[p] A) \triangleright \langle \emptyset; 0 \rangle \quad \text{By rule ret} \]
\[ D \text{ reads } R_D \text{ writes } W_D \text{ and } W_D = \{p\} \quad \text{By Def. 6.2} \]
\[ n \in X \quad \text{Above} \]
\[ M(n) \in M(X) \quad \text{Name term application is pointwise} \]
\[ M(n) \in W \quad \text{By above equality} \]
\[ M(n) = p \]
\[ \{p\} \subseteq W \quad \text{By set theory} \]
\[ \langle W_D; R_D \rangle \leq \langle W; R \rangle \]

- **Case**

\[ \Gamma_1 \vdash^M e_1 : (F A \triangleright e_1) \quad \Gamma_1, x : A \vdash^M e_2 : (C \triangleright e_2) \]
\[ \Gamma_1 \vdash^M \text{let}(e_1, x.e_2) : C \triangleright (e_1 \text{ then } e_2) \quad \text{let} \]

, Vol. 1, No. 1, Article . Publication date: May 2021.
\[
\begin{align*}
\Gamma \vdash \text{let } t_1 : \Gamma_1 & \quad \text{Given} \\
S_1 : \Gamma_1 \vdash M \ e_1 : FA \triangleright e_1 & \quad \text{Subderivation 1 of } S \\
D_1 : S_1 \vdash^M_{t_1} e_1 \Downarrow S_{12}; t_1 & \quad \text{Subderivation 1 of } D \\
\quad \exists \Gamma_{12} \supseteq \Gamma_1 \text{ such that } S_{12} : \Gamma_{12} & \quad \text{By i.h. on } S_1 \\
\quad \Gamma_{12} \vdash \text{let } t_1 : FA \triangleright \langle \emptyset; \emptyset \rangle & \quad " \\
\quad D_1 \text{ reads } R_{D_1} \text{ writes } W_{D_1} & \quad " \\
\quad \langle W_{D_1}; R_{D_1} \rangle \leq e_1 & \quad " \\
\quad \langle W_{D_1}; R_{D_1} \rangle \leq \langle W_1, R_1 \rangle & \quad " \\
\quad \Gamma_{12} \vdash v : A & \quad \text{inversion of typing rule } \text{ret}, \text{ for terminal computation } t_1 \\
\end{align*}
\]

\[
\begin{align*}
\Gamma, x : A \vdash M \ e_2 : C \triangleright e_2 & \quad \text{Subderivation 2 of } S \\
\quad \Gamma_{12}, x : A \vdash^M \ e_2 : C \triangleright e_2 & \quad \text{Lemma B.2 (Weakening)} \\
\quad \Gamma_{12} \vdash^M [v/x]e_2 : C \triangleright e_2 & \quad \text{Lemma B.3 (Substitution)} \\
D_2 : S_{12} \vdash^M [v/x]e_2 \Downarrow S_{2}; t_2 & \quad \text{Subderivation 2 of } D \\
\quad \exists \Gamma_{12} \supseteq \Gamma_1 \text{ such that } & \quad \text{By i.h. on } S_2 \\
\quad \Gamma_{12} \vdash S_2 : \Gamma_2 & \quad " \\
\quad \Gamma_{12} \vdash t_2 : C \triangleright \langle \emptyset; \emptyset \rangle & \quad " \\
\quad D_2 \text{ reads } R_{D_2} \text{ writes } W_{D_2} & \quad " \\
\quad \langle W_{D_2}; R_{D_2} \rangle \leq e_2 & \quad " \\
\quad \langle W_{D_2}; R_{D_2} \rangle \leq \langle W_2, R_2 \rangle & \quad " \\
\end{align*}
\]

\[
\Gamma, x : \emptyset \vdash \langle \emptyset \rangle \quad W_1 \perp W_2 \text{ and } R_1 \perp W_2 & \quad \text{Definition of } e_1 \text{ then } e_2 \\
\Gamma, x : \emptyset \vdash \langle \emptyset \rangle \quad W_{D_1} \perp W_{D_2} \text{ and } R_{D_1} \perp W_{D_2} & \quad W_{D_1} \subseteq W_{D_2} ; W_{D_2} \subseteq W_2 ; R_{D_1} \subseteq R_1 \\
\Gamma, x : \emptyset \vdash \langle \emptyset \rangle \quad W_D = W_{D_1} \perp W_{D_2} & \quad \text{By Def. 6.2} \\
\Gamma, x : \emptyset \vdash \langle \emptyset \rangle \quad W_D = R_{D_1} \cup (R_{D_2} - W_{D_1}) & \quad " \\
\Gamma, x : \emptyset \vdash \langle \emptyset \rangle \quad D \text{ reads } R_D \text{ writes } W_D & \quad " \\
\Gamma, x : \emptyset \vdash \langle \emptyset \rangle \quad \langle W_D, R_D \rangle = \langle W, R \rangle & \quad \text{Since } W_D \subseteq W \text{ and } R_D \subseteq R \\
\end{align*}
\]

- **Case** 
  \[
\begin{align*}
\Gamma \vdash^M \ e : (A \rightarrow E) \triangleright e_1 & \quad \Gamma \vdash v : A \\
\quad \Gamma \vdash^M (e \ v) : (E \text{ after } e_1) & \quad \text{app} \\
\end{align*}
\]
  Similar to the case for let.

- **Case** 
  \[
\begin{align*}
\Gamma \vdash^M \ v : (A_1 \times A_2) & \quad \Gamma, x_1 : A_1, x_2 : A_2 \vdash^M \ e : E \\
\quad \Gamma \vdash^M \text{split}(\langle v, x_1.x_2.e \rangle) : E & \quad \text{split} \\
\end{align*}
\]
  Similar to the case for let, using Lemma B.8 (Canonical Forms).

- **Case** 
  \[
\begin{align*}
\Gamma, x_1 : A_1 \vdash^M \ e_1 : E & \quad \Gamma, x_2 : A_2 \vdash^M \ e_2 : E \\
\quad \Gamma \vdash^M \text{case}(\langle v, x_1.e_1, x_2.e_2 \rangle) : E & \quad \text{case} \\
\end{align*}
\]
  Similar to the case for let, using Lemma B.8 (Canonical Forms).

- **Case** 
  \[
\begin{align*}
\Gamma \vdash v_M : (Nm \rightarrow Nm)[M] & \quad \Gamma \vdash v : Nm[M] \\
\quad \Gamma \vdash (v_M \ v) : F(Nm[M]) \triangleright \langle \emptyset; \emptyset \rangle & \quad \text{name-app} \\
\end{align*}
\]

\]
\[ \Gamma_1 \vdash v : Nm[i] \quad \text{Given} \]
\[ v = \text{name } n \quad \text{Lemma B.8 (Canonical Forms)} \]
\[ \Gamma \vdash n \in i \quad \text{Above} \]
\[ M \Downarrow_M \lambda a. M' \quad \text{By inversion on } \Downarrow (\text{name-app}) \]
\[ \Downarrow_M p \quad \text{By a property of } \Downarrow_M \]
\[ p = \beta (\lambda a. M')(n) \quad \text{By a property of } =_\beta \]
\[ (\Gamma_2 = \Gamma_1), (S_2 = S_1) \quad \text{Suppose} \]
\[ \vdash S_2 : \Gamma_2 \quad \text{By above equalities and } S_1 \vdash \Gamma_1 \]
\[ \Gamma_1 \vdash \text{name } p : Nm[M(i)] \quad \text{By rule name} \]
\[ \vdash (R_D = R = \emptyset), (W_D = W = \emptyset) \quad \text{By above equalities} \]

**Case**

\[ \Gamma_1, a : \gamma, P \vdash^M t : E \]
\[ \Downarrow_M t : (\forall a : \gamma \mid P, E) \quad \text{AllIndexIntro} \]

\[ \mathcal{S}_0 :: \Gamma_1, a : \gamma, P \vdash^M t : E \quad \text{Subderivation} \]
\[ \mathcal{D}_0 :: S_1 \vdash^M e \Downarrow S_2 ; t \quad \text{Subderivation} \]
\[ \exists \Gamma_2 \subseteq \Gamma_1 \quad \text{By i.h.} \]
\[ \vdash S_2 : \Gamma_2 \quad \text{''} \]
\[ \mathcal{D}_0 \text{ reads } R_{\mathcal{D}_0} \text{ writes } W_{\mathcal{D}_0} \quad \text{''} \]
\[ \Gamma_2 \vdash t : E \quad \text{''} \]
\[ \langle R_{\mathcal{D}_0} ; W_{\mathcal{D}_0} \rangle \leq \langle R ; W \rangle \quad \text{''} \]
\[ \vdash \mathcal{D} \text{ reads } R_{\mathcal{D}} \text{ writes } W_{\mathcal{D}} \quad \text{By Def. 6.2} \]
\[ \langle R_{\mathcal{D}} ; W_{\mathcal{D}} \rangle \leq \langle R ; W \rangle \quad \text{By set theory} \]

**Case**

\[ \Gamma_1 \vdash i : \gamma \]
\[ \Gamma_1 \vdash^M e : (\forall a : \gamma \mid P, E) \quad \text{extract}(\Gamma_1) \vdash [i/a]P \]
\[ \Downarrow_M e : [i/a]E \quad \text{AllIndexElim} \]
\[ S_0 :: \quad \Gamma_1 \vdash^M \text{e} : (\forall \alpha : \gamma. E) \quad \text{Subderivation} \]
\[ D_0 :: \quad S_1 \vdash^m \text{e} \Downarrow S_2 ; t \quad \text{Subderivation} \]
\[ \exists \Gamma_2 \subseteq \Gamma_1 \quad \text{By i.h.} \]
\[ \quad \vdash S_2 : \Gamma_2 \quad " \]
\[ D_0 \text{ reads } R_{D_0} \text{ writes } W_{D_0} " \]
\[ \Gamma_2 \vdash t : (\forall \alpha : \gamma. E) " \]
\[ \langle R_{D_0}; W_{D_0} \rangle \preceq \langle R; W \rangle " \]
\[ \Gamma_1 \vdash \text{i} : \gamma \quad \text{Subderivation} \]
\[ \Gamma_2 \vdash \text{i} : \gamma \quad \text{By weakening} \]
\[ \quad \vdash \text{e} : \lambda \rangle \quad \text{By typing rule} \]
\[ \quad \vdash D \text{ reads } R_D \text{ writes } W_D \quad \text{By Def. 6.2} \]
\[ \langle R_D; W_D \rangle \preceq \langle R; W \rangle \quad \text{By set theory} \]

- **Case**
  \[ \Gamma, \alpha : K \vdash^M \text{t} : E \quad \text{AllIntro} \]
  \[ \Gamma \vdash^M \text{t} : (\forall \alpha : K. E) \] Similar to the AllIndexIntro case.

- **Case**
  \[ \Gamma \vdash^M \text{e} : (\forall \alpha : K. E) \quad \Gamma \vdash A : K \quad \text{AllElim} \]
  \[ \Gamma \vdash^M \text{e} : [A/\alpha]E \] Similar to the AllIndexElim case.

\[ \square \]

C  BIDIRECTIONAL TYPING

C.1 Syntax
As discussed below, bidirectional typing requires some annotations, so we assume that values \( v \) and expressions \( e \) have been extended with annotations \( (v : A) \) and \( (e : A) \). We also assume that we have explicit syntactic forms \( e[i] \) and \( e[A] \), which avoid guessing quantifier instantiations.

C.2 Bidirectional Typing Rules
The typing rules in Figures 13 and 14 are declarative: they define what typings are valid, but not how to derive those typings. The rules’ use of names and effects annotations means that standard unification-based techniques, like Damas–Milner inference, are not readily applicable.

Following the DML tradition, we obtain an algorithmic version of our typing rules by defining a bidirectional system [Pierce and Turner 2000]: we split judgments with a colon into judgments with an arrow. Thus, the computation typing judgment \( \cdots \vdash \text{e} : E \) becomes two judgments. The first is the checking judgment \( \Gamma \vdash^M \text{e} \subseteq E \), in which the type \( E \) is already known—it is an input to the algorithm. The second is the synthesis judgment \( \Gamma \vdash^M \text{e} \Rightarrow E \), in which \( E \) is not known—it is an output—and the rules construct \( E \) by examining \( e \) (and \( \Gamma \)).

In formulating the bidirectional versions of value and computation typing (Figures 22 and 23), we mostly follow the “recipe” of Dunfield and Pfening [2004]: introduction rules check, and elimination rules synthesize. More precisely, the principal judgment—the judgment, either a premise or conclusion, that has the connective being introduced or eliminated—is checking (\( \subseteq \)) for introduction rules, and synthesizing (\( \Rightarrow \)) for elimination rules. In many cases, once the direction of that premise (or conclusion) is determined, the direction of the other judgments follows by considering what information is known (as input, or as the output type of the principal judgment, if that judgment is synthesizing). For example, if we commit to checking the conclusion of echk-lam,
we should check the premise because its type is a subexpression of the type in the conclusion. (Checking is more powerful than synthesis: every expression that synthesizes also checks, but not all expressions that check can synthesize.)

When a synthesis (elimination) premise attempts to type an expression that is a checking (introduction) form, the programmer must write a type annotation \( (e : E) \). Thus, following the recipe means that we have a straightforward annotation discipline: annotations are needed only on redexes. While we could reduce the number of annotations by adding synthesis rules—for example, allowing the unit value \( () \) to synthesize unit—this makes the system larger without changing its essential properties; for a discussion of the implications of such extensions in a different context, see Dunfield and Krishnaswami [2013].

Dually, when an expression synthesizes but we are trying to derive a checking judgment, we use (1) vchk-sub for value typing, or (2) echk-sub for computation typing. The latter rule includes effect subsumption.

D BIDIRECTIONAL TYPING PROOFS

THEOREM D.1 (Soundness of Bidirectional Value Typing).
Fig. 23. Bidirectional computation typing

(1) If \( \Gamma \vdash v \Rightarrow A \), then there exists a value \( v' \) such that \( \Gamma \vdash v' : A \) and \( |v| = v' \).
(2) If \( \Gamma \vdash v \Leftarrow A \), then there exists a value \( v' \) such that \( \Gamma \vdash v' : A \) and \( |v| = v' \).

Proof. By induction on the given derivation.

Part (1): Proceed by cases on the rule concluding \( \Gamma \vdash v \Rightarrow A \).
Case \( (x : A) \in \Gamma \)
\[ \Gamma \vdash x \Rightarrow A \]

\( (x : A) \in \Gamma \)

*Given*

\( \Gamma \vdash x : A \)

*By rule var*

\(|x| = x \)

*By definition of \(|-|\)*

\( \Rightarrow \Gamma \vdash v' : A \) and \(|v| = v' \)

*where \( v' = x \) and \( v = x \)*

Case \( \Gamma \vdash v_1 \Leftarrow A \)

\[ \Gamma \vdash (v_1 : A) \Rightarrow A \]

By inductive hypothesis

\(|v_1| = v'_1 \)

*By definition of \(|-|\)*

\( \Rightarrow \Gamma \vdash v' : \) and \(|v| = v' \)

*where \( v' = v'_1 \) and \( v = (v_1 : A) \)*

Part (2): Proceed by cases on the rule concluding \( \Gamma \vdash v \Leftarrow A \).

Case \( \Gamma \vdash v_1 \Leftarrow A_1 \)

\[ \Gamma \vdash (v_1, v_2) \Leftarrow (A_1 \times A_2) \]

By inductive hypothesis

\(|v_1| = v'_1 \)

*By inductive hypothesis*

\(|v_2| = v'_2 \)

*By rule pair*

\(|(v_1, v_2)| = (|v_1|, |v_2|) = (v'_1, v'_2) \)

*By definition of \(|-|\)*

\( \Rightarrow \Gamma \vdash v' : (A_1 \times A_2) \) and \(|v| = v' \)

*where \( v' = (v'_1, v'_2) \) and \( v = (v_1, v_2) \)*

Case \( \Gamma \vdash n \in X \)

\[ \Gamma \vdash (\text{name } n) \Leftarrow \text{Nm}[X] \]

\( \Gamma \vdash n \in X \)

*Given*

\( \Gamma \vdash (\text{name } n) : \text{Nm}[X] \)

*By rule name*

\(|(\text{name } n)| = (\text{name } n) \)

*By definition of \(|-|\)*

\( \Rightarrow \Gamma \vdash v' : \text{Nm}[X] \) and \(|v| = v' \)

*where \( v' = (\text{name } n) \) and \( v = (\text{name } n) \)*

Case \( \Gamma \vdash M_v \Rightarrow (\text{Nm } \text{Nm}[X]) \)

\[ \Gamma \vdash (\text{nmfn } M_v) \Leftarrow (\text{Nm } \text{Nm}[X])[M] \]

*By \( \beta \)-reduction*
∃ M′ such that Γ ⊢ M′ : (Nm Nm) and |Mv| = M′ By i.h.
Mv =β M Given
|Mv| =β M Type erasure does not affect convertibility
M′ =β M Since |Mv| = M′
Γ ⊢ (nmfn Mv) : (Nm Nm) By rule name
|nmfn Mv| = (nmfn |Mv|) = (nmfn M′v)
By definition of |−|
and |Mv| = M′v
Γ ⊢ v′ : (Nm Nm) and |v| = v′
where v′ = (nmfn M′v)
and v = (nmfn Mv)

• Case

Γ ⊢ n ∈ X Γ(n) = A vchk-ref
Γ ⊢ (ref n) ≫ Ref[X] A

Γ ⊢ n ∈ X Given
Γ(n) = A Given
Γ ⊢ (ref n) : Ref[X] A By rule ref
|ref n| = ref n By definition of |−|
Γ ⊢ v′ : Ref[X] A and |v| = v′ where v′ = (ref n)
and v = (ref n)

• Case

Γ ⊢ n ∈ X Γ(n) = E vchk-thunk
Γ ⊢ (thunk n) ≫ (Thk[X] E)

Γ ⊢ n ∈ X Given
Γ(n) = E Given
Γ ⊢ (thunk n) : Thk[X] E By rule thunk
|(thunk n)| = thunk n By definition of |−|
Γ ⊢ v′ : Thk[X] E and |v| = v′ where v′ = (thunk n)
and v = (thunk n)

• Case

Γ ⊢ v1 ⇒ A1 Γ ⊢ A1 ⊆ v A2 vchk-sub
Γ ⊢ v1 ≫ A2

By i.h. and vtype-sub.

□

Theorem D.2 (Completeness of Bidirectional Value Typing). If Γ ⊢ v : A then there exist values v′ and v″ such that
(1) Γ ⊢ v′ ⇒ A and |v′| = v
(2) Γ ⊢ v″ ≫ A and |v″| = v

Proof. By induction on the derivation of Γ ⊢ v : A.

Case

Γ ⊢ () : unit
Case \((x : A) \in \Gamma\)

\[\Gamma \vdash x : A\] var

\(\Gamma \vdash x \Rightarrow A\) \hspace{1cm} By rule vsyn-var
\(|x| = x\) \hspace{1cm} By definition of \([-]\)

\(\Gamma \vdash v' \Rightarrow A\) and \(|v'| = v\) \hspace{1cm} where \(v' = x\) and \(v = x\)

\(\Gamma \vdash x \Leftarrow A\) \hspace{1cm} By rule vchk-conv

\(\Gamma \vdash v'' \Leftarrow A\) and \(|v''| = v\) \hspace{1cm} where \(v'' = x\) and \(v = x\)

\(\\) and \(|x| = x\)

Case \(\Gamma \vdash v_1 : A_1, \Gamma \vdash v_2 : A_2\)

\[\Gamma \vdash (v_1, v_2) : (A_1 \times A_2)\] pair

\(\exists v_1''\) such that \(\Gamma \vdash v_1'' \Leftarrow A_1\) and \(|v_1''| = v_1\) \hspace{1cm} By inductive hypothesis

\(\exists v_2''\) such that \(\Gamma \vdash v_2'' \Leftarrow A_2\) and \(|v_2''| = v_2\) \hspace{1cm} By inductive hypothesis

\(\Gamma \vdash (v_1'', v_2'') \Leftarrow (A_1 \times A_2)\) \hspace{1cm} By rule vchk-pair

\(|(v_1'', v_2'')| = (|v_1''|, |v_2''|) = (v_1, v_2)\) \hspace{1cm} By definition of \([-]; |v_1''| = v_1; |v_2''| = v_2\)

\(\Gamma \vdash v'' \Leftarrow (A_1 \times A_2)\) and \(|v''| = v\) \hspace{1cm} where \(v'' = (v_1'', v_2'')\) and \(v = (v_1, v_2)\)

\(\Gamma \vdash (v_1'', v_2'') : (A_1 \times A_2) \Rightarrow (A_1 \times A_2)\) \hspace{1cm} By rule vsyn-anno

\(|(v_1'', v_2'') : (A_1 \times A_2)| = |(v_1'', v_2'')| = (v_1, v_2)\) \hspace{1cm} By definition of \([-]; |(v_1'', v_2'')| = (v_1, v_2)\)

\(\Gamma \vdash v' \Rightarrow (A_1 \times A_2)\) and \(|v'| = v\) \hspace{1cm} where \(v' = (v_1'', v_2'')\) and \(v = (v_1, v_2)\)

Case \(\Gamma \vdash n \in X\)

\[\Gamma \vdash (\text{name } n) : \text{Nm}[X]\] name

\(\Gamma \vdash n \in X\) \hspace{1cm} Given

\[\Gamma \vdash (\text{name } n) \Leftarrow \text{Nm}[X]\] \hspace{1cm} By rule vchk-name

\(|\text{(name } n)| = (\text{name } n)\) \hspace{1cm} By definition of \([-]\)

\(\Gamma \vdash v'' \Leftarrow \text{Nm}[X]\) and \(|v''| = v\) \hspace{1cm} where \(v'' = (\text{name } n)\) and \(v = (\text{name } n)\)

\(\Gamma \vdash (\text{name } n : \text{Nm}[X]) \Rightarrow \text{Nm}[X]\) \hspace{1cm} By rule vsyn-anno

\(|\text{name } n : \text{Nm}[X])| = |(\text{name } n)| = (\text{name } n)\) \hspace{1cm} By definition of \([-]\)

\(\Gamma \vdash v' \Rightarrow \text{Nm}[X]\) and \(|v'| = v\) \hspace{1cm} where \(v' = (\text{name } n : \text{Nm}[X])\) and \(v = (\text{name } n)\)

Case \(\Gamma \vdash M_v : (\text{Nm } \Rightarrow \text{Nm})\)

\[M_v =_{\beta} M\] namefn

\(\Gamma \vdash (\text{nmfn } M_v) : (\text{Nm } \Rightarrow \text{Nm})[M]\)
∃ M′ such that

\[ \Gamma \vdash M′ \Rightarrow (\text{Nm} \Rightarrow \text{Nm}) \] and [M′] = M

By inductive hypothesis

\[ M\in M \] Given

\[ [M′] = M \] Since [M′] = M

\[ M′ = M \] Type annotation does not affect convertibility

\[ \Gamma \vdash (\text{nmfn} M′) \Leftarrow (\text{Nm} \Rightarrow \text{Nm})[M] \] By rule vchk-namefn

\[ ([\text{nmfn} M′] = (\text{nmfn} [M′]) = (\text{nmfn} M) \] By definition of |−|

\[ and [M′] = M \]

\[ \Gamma \vdash v′′ \Leftarrow (\text{Nm} \Rightarrow \text{Nm})[M] \] and [v′′] = v

where v′′ = (\text{nmfn} M′) and v = (\text{nmfn} M)

\[ \Gamma \vdash (\text{nmfn} M′ : (\text{Nm} \Rightarrow \text{Nm})[M]) \Rightarrow (\text{Nm} \Rightarrow \text{Nm})[M] \] By rule vsyn-anno

\[ ([\text{nmfn} M′ : (\text{Nm} \Rightarrow \text{Nm})[M])] = (\text{nmfn} M) \] By definition of |−|

\[ \Gamma \vdash v′ \Rightarrow (\text{Nm} \Rightarrow \text{Nm})[M] \] and [v′] = v

where v′ = (\text{nmfn} M′ : (\text{Nm} \Rightarrow \text{Nm})[M])

Case

\[ \Gamma \vdash n \in X \quad \Gamma(n) = A \]

\[ \Gamma \vdash (\text{ref } n) : \text{Ref}[X] \Rightarrow A \] ref

\[ \Gamma \vdash n \in X \]

\[ \Gamma(n) = A \] Given

\[ \Gamma \vdash (\text{ref } n) \Leftarrow \text{Ref}[X] \Rightarrow A \] By rule vchk-ref

\[ ([\text{ref } n]) = (\text{ref } n) \] By definition of |−|

\[ \Gamma \vdash v′′ \Leftarrow \text{Ref}[X] \Rightarrow A \] and [v′′] = v

where v′′ = (\text{ref } n) and v = (\text{ref } n)

\[ \Gamma \vdash (\text{ref } n) \Rightarrow \text{Ref}[X] \Rightarrow A \] By rule vsyn-anno

\[ ([\text{ref } n : \text{Ref}[X]]) = (\text{ref } n) \] By definition of |−|

\[ \Gamma \vdash v′ \Rightarrow \text{Ref}[X] \Rightarrow A \] and [v′] = v

Case

\[ \Gamma \vdash n \in X \quad \Gamma(n) = E \]

\[ \Gamma \vdash (\text{thunk } n) : (\text{Thk}[X] \Rightarrow E) \] thunk

\[ \Gamma \vdash n \in X \]

\[ \Gamma(n) = E \] Given

\[ \Gamma \vdash (\text{thunk } n) \Leftarrow (\text{Thk}[X] \Rightarrow E) \] By rule vchk-thunk

\[ ([\text{thunk } n]) = (\text{thunk } n) \] By definition of |−|

\[ \Gamma \vdash v′′ \Leftarrow (\text{Thk}[X] \Rightarrow E) \] and [v′′] = v

where v′′ = (\text{thunk } n) and v = (\text{thunk } n)

\[ \Gamma \vdash (\text{thunk } n : (\text{Thk}[X] \Rightarrow E)) \Rightarrow (\text{Thk}[X] \Rightarrow E) \] By rule vsyn-anno

\[ ([\text{thunk } n : (\text{Thk}[X] \Rightarrow E)]) = \text{thunk } n \] By definition of |−|

\[ \Gamma \vdash v′ \Rightarrow (\text{Thk}[X] \Rightarrow E) \] and [v′] = v

where v′ = (\text{thunk } n : (\text{Thk}[X] \Rightarrow E)) and v = (\text{thunk } n)

\[ \square \]

Theorem D.3 (Soundness of Bidirectional Computation Typing).

1. If \( \Gamma \vdash^E e \Rightarrow E \), then there exists a value \( e′ \) such that \( \Gamma \vdash^E e′ : E \text{ and } \vert e \vert = e′ \)

2. If \( \Gamma \vdash^E e \Leftarrow E \), then there exists a value \( e′ \) such that \( \Gamma \vdash^E e′ : E \text{ and } \vert e \vert = e′ \)
**Proof.** By induction on the given derivation.

Part (1): Proceed by case analysis on the rule concluding $\Gamma \vdash^M e \Rightarrow E$.

- **Case**

  $\Gamma \vdash^M e_1 \Rightarrow ((A \rightarrow E) \triangleright e_1) \quad \Gamma \vdash \nu \leftarrow A \quad \text{syn-app}$

  $\Gamma \vdash^M (e_1 \nu) \Rightarrow (E \text{ after } e_1)$

  $\Gamma \vdash^M e_1' : ((A \rightarrow E) \triangleright e_1)$ and $|e_1| = e_1'$

  By inductive hypothesis

  $\Gamma \vdash \nu' : A$ and $|\nu| = \nu'$

  By Thm. D.1

  $\Gamma \vdash^M (e_1' \nu') : (E \text{ after } e_1)$

  By rule app

  $|e_1| = |e_1'| = (e_1' \nu')$

  By definition of $\triangleright$

  $\Gamma \vdash^M e' : (E \text{ after } e_1)$ and $|e| = e'$

  where $e' = (e_1' \nu')$ and $e = (e_1 \nu)$

- **Case**

  $\Gamma \vdash \nu \Rightarrow \text{Thk}[X] \ (C \triangleright e) \quad \text{syn-force}$

  $\Gamma \vdash^M \text{force}(\nu) \Rightarrow (C \triangleright (\emptyset; X \text{ then } e))$

  $\Gamma \vdash \nu' : \text{Thk}[X] \ (C \triangleright e)$ and $|\nu| = \nu'$

  By Thm. D.1

  $\Gamma \vdash^M \text{force}(\nu') : (C \triangleright (\emptyset; X \text{ then } e))$

  By rule force

  $|\text{force}(\nu)| = |\text{force}(\nu')| = |\text{force}(\nu')|$

  By definition of $\triangleright$

  and $|\nu| = \nu'$

  $\Gamma \vdash^M e' : (C \triangleright (\emptyset; X \text{ then } e))$ and $|e| = e'$

  where $e' = \text{force}(\nu')$ and $e = \text{force}(\nu)$

- **Case**

  $\Gamma \vdash \nu \Rightarrow \text{Ref}[X] A \quad \text{syn-get}$

  $\Gamma \vdash^M \text{get}(\nu) \Rightarrow (F A) \triangleright (\emptyset; X)$

  $\Gamma \vdash \nu' : \text{Ref}[X] A$ and $|\nu| = \nu'$

  By Thm. D.1

  $\Gamma \vdash^M \text{get}(\nu') : (F A) \triangleright (\emptyset; X)$

  By rule get

  $|\text{get}(\nu)| = |\text{get}(\nu)| = |\text{get}(\nu')|$

  By the definition of $\triangleright$

  and $|\nu| = \nu'$

  $\Gamma \vdash^M e' : (F A) \triangleright (\emptyset; X)$ and $|e| = e'$

  where $e' = \text{get}(\nu')$ and $e = \text{get}(\nu)$

- **Case**

  $\Gamma \vdash \nu_M \Rightarrow (\text{Nm}\stackrel{\text{syn}}{\Rightarrow} \text{Nm})[M] \quad \text{syn-name-app}$

  $\Gamma \vdash \nu \Rightarrow \text{Nm}[i]$

  $\Gamma \vdash^M (\nu_M \nu) \Rightarrow F (\text{Nm}[\text{M}(i)]) \triangleright (\emptyset; \emptyset)$

  $\Gamma \vdash \nu_M' : (\text{Nm}\stackrel{\text{syn}}{\Rightarrow} \text{Nm})[M]$ and $|\nu_M| = \nu_M'$

  By Thm. D.1

  $\Gamma \vdash \nu' : \text{Nm}[i]$ and $|\nu| = \nu'$

  By Thm. D.1

  $\Gamma \vdash^N (\nu_M' \nu') : F (\text{Nm}[\text{M}(i)]) \triangleright (\emptyset; \emptyset)$

  By rule name-app

  $|(\nu_M \nu)| = (|\nu_M| |\nu|) = (\nu_M' \nu')$

  By definition of $\triangleright$; $|\nu_M| = \nu_M'$; $|\nu| = \nu'$

  $\Gamma \vdash^M e' : F (\text{Nm}[\text{M}(i)]) \triangleright (\emptyset; \emptyset)$ and $|e| = e'$

  where $e' = (\nu_M' \nu')$ and $e = (\nu_M \nu)$

- **Case**

  $\Gamma \vdash^M e \Rightarrow (\forall a : \gamma, E) \quad \Gamma \vdash i : \gamma \quad \text{syn}$

  $\Gamma \vdash^M e[i] \Rightarrow [i/\alpha]E$
\[
\Gamma \vdash M : (\forall \alpha : \gamma. E) \quad \text{and} \quad |e| = e' \\
\Gamma \vdash i : \gamma \quad \text{Given} \\
\vdash e[i] = |e'| \quad \text{By } |e| = e' \\
\vdash \Gamma ; e' : [i/a]E \quad \text{By rule AllIndexElim}
\]

- **Case**
  \[
  \begin{align*}
  \Gamma &\vdash M : (\forall \alpha : K. E) \\
  \Gamma &\vdash A : K \\
  \Gamma ; e' &: [\alpha/a]E \\
  \end{align*}
  \]

  By i.h. and rule etype-sub.

- **Case**
  \[
  \begin{align*}
  \Gamma &\vdash v \Rightarrow (A_1 \times A_2) \\
  \Gamma, x_1 : A_1, x_2 : A_2 &\vdash M e_1 \iff E \\
  \Gamma, x_1 &\vdash M e_2 \iff E \\
  \end{align*}
  \]

  By Thm. D.1

  By i.h. and rule etype-sub.

- **Case**
  \[
  \begin{align*}
  \Gamma &\vdash v \Rightarrow (A_1 + A_2) \\
  \Gamma, x_1 : A_1, x_2 : A_2 &\vdash M e_1 \iff E \\
  \Gamma, x_1 &\vdash M e_2 \iff E \\
  \end{align*}
  \]

  By i.h. and rule etype-sub.

Part (2): Proceed by case analysis on the rule concluding \( \Gamma \vdash M e \iff E \).

- **Case**
  \[
  \begin{align*}
  \Gamma &\vdash M e \Rightarrow (C \supset e_1) \\
  \end{align*}
  \]

  By i.h. and rule etype-sub.
\[
\Gamma \vdash v' : (A_1 + A_2) \text{ and } |v| = v' \quad \text{By Thm. D.1} \\
\Gamma, x_1 : A_1 \vdash M_{e'} : E \text{ and } |e_1| = e'_1 \quad \text{By inductive hypothesis} \\
\Gamma, x_2 : A_2 \vdash M_{e'_2} : E \text{ and } |e_2| = e'_2 \quad \text{By inductive hypothesis} \\
\Gamma \vdash M_{\text{case}(v', x_1.e'_1, x_2.e'_2)} : E \quad \text{By rule case} \\
|\text{case}(v, x_1.e_1, x_2.e_2)| = |\text{case}(v, x_1.e_1, x_2.e_2)| \quad \text{By definition of } \left|{-}\right| \\
= \text{case}(v', x_1.e'_1, x_2.e'_2) \quad \text{Since } |v| = v', |e_1| = e'_1, |e_2| = e'_2 \\
\Rightarrow \Gamma \vdash M_{e'} : E \text{ and } |e| = e' \quad \text{where } e' = \text{case}(v', x_1.e'_1, x_2.e'_2) \\
\text{and } e = \text{case}(v, x_1.e_1, x_2.e_2)
\]

\* Case

\[
\Gamma \vdash v \iff A \\
\Gamma \vdash \text{ret}(v) \iff \left((\text{F} A) \triangleright \langle \emptyset; \emptyset \rangle \right) \quad \text{echk-ret} \\
\Gamma \vdash v' : A \text{ and } |v| = v' \quad \text{By Thm. D.1} \\
\Gamma \vdash \text{ret}(v') : \left((\text{F} A) \triangleright \langle \emptyset; \emptyset \rangle \right) \quad \text{By rule ret} \\
|\text{ret}(v)| = |\text{ret}(v)| = |\text{ret}(v')| \quad \text{By definition of } \left|{-}\right| \text{ and } |v| = v' \\
\Rightarrow \Gamma \vdash M_{e'} : \left((\text{F} A) \triangleright \langle \emptyset; \emptyset \rangle \right) \text{ and } |e| = e' \quad \text{where } e' = \text{ret}(v') \text{ and } e = \text{ret}(v)
\]

\* Case

\[
\Gamma \vdash M_{e_1} \Rightarrow (A) \triangleright e_1 \quad \Gamma, x : A \vdash M_{e_2} \iff (C \triangleright e_2) \quad \text{echk-let} \\
\Gamma \vdash \text{let}(e_1, x.e_2) \iff (C \triangleright (e_1 \text{ then } e_2)) \\
\Gamma \vdash M_{e'_1} : (A) \triangleright e_1 \text{ and } |e_1| = e'_1 \quad \text{By inductive hypothesis} \\
\Gamma, x : A \vdash M_{e'_2} : (C \triangleright e_2) \text{ and } |e_2| = e'_2 \quad \text{By inductive hypothesis} \\
\Gamma \vdash M_{\text{let}(e'_1, x.e'_2)} : (C \triangleright (e_1 \text{ then } e_2)) \quad \text{By rule let} \\
|\text{let}(e_1, x.e_2)| = |\text{let}(e_1, x.e_2)| \quad \text{By definition of } \left|{-}\right| \\
= \text{let}(e'_1, x.e'_2) \quad \text{Since } |e_1| = e'_1, |e_2| = e'_2 \\
\Rightarrow \Gamma \vdash M_{e'} : \left(C \triangleright (e_1 \text{ then } e_2) \right) \text{ and } |e| = e' \quad \text{where } e' = \text{let}(e'_1, x.e'_2) \\
\text{and } e = \text{let}(e_1, x.e_2)
\]

\* Case

\[
\Gamma, x : A \vdash M_{e_1} \iff E \\
\Gamma \vdash \text{(A \rightarrow E) \triangleright (\emptyset; \emptyset)} \quad \text{echk-lam} \\
\Gamma, x : A \vdash M_{\text{let}(e_1)} \iff ((A \rightarrow E) \triangleright (\emptyset; \emptyset)) \quad \text{By rule lam} \\
|\text{(A \rightarrow e_1)}| = (\text{A \rightarrow e_1}) = (\text{A \rightarrow e_1}) \quad \text{By definition of } \left|{-}\right| \text{ and } |e_1| = e'_1 \\
\Rightarrow \Gamma \vdash M_{e'} : \left((A \rightarrow E) \triangleright (\emptyset; \emptyset) \right) \text{ and } |e| = e' \quad \text{where } e' = \text{(A \rightarrow e_1)} \text{ and } e = (\text{A \rightarrow e_1}) \\
\]

\* Case

\[
\Gamma \vdash v \iff \text{Nm}[X] \quad \Gamma \vdash M_{e_1} \iff E \quad \text{echk-thunk} \\
\Gamma \vdash \text{thunk}(v, e_1) \iff (\text{F Thk}[M(X)] E_1) \triangleright \langle M(X); \emptyset \rangle
\]

, Vol. 1, No. 1, Article . Publication date: May 2021.
Let E = \((F(Thk[M(X)])E_1)) \triangleright (M(X); \emptyset)\) Assumption

\(\exists v' \text{ such that } \Gamma \vdash v': \text{Nm}[X] \text{ and } |v| = v'\) By Thm. D.1

\(\exists e'_1 \text{ such that } \Gamma \vdash E\text{ and } |e_1| = e'_1\) By inductive hypothesis

\(\Gamma \vdash \text{thunk}(v', e'_1) : E\) By rule thunk

\(|\text{thunk}(v, e_1)| = \text{thunk}(|v|, |e_1|) = \text{thunk}(v', e'_1)\) By definition of \(|\cdot|\)

\(\text{Case } \Gamma \vdash \text{M} e' : E \text{ and } |e| = e' \text{ where } e' = \text{thunk}(v', e'_1)\) and \(e = \text{thunk}(v, e_1)\)

- Case \(\Gamma \vdash v_1 \iff \text{Nm}[X] \quad \Gamma \vdash v_2 \iff A\) echk-ref

\(\exists v'_1 \text{ such that } \Gamma \vdash v'_1 : \text{Nm}[X] \text{ and } |v_1| = v'_1\) By Thm. D.1

\(\exists v'_2 \text{ such that } \Gamma \vdash v'_2 : A \text{ and } |v_2| = v'_2\) By Thm. D.1

\(\Gamma \vdash \text{ref}(v'_1, v'_2) : (F(\text{Ref}[M(X)]A)) \triangleright (M(X); \emptyset)\) By rule ref

\(|\text{ref}(v_1, v_2)| = |\text{ref}(v'_1, v'_2)| = |\text{ref}(v'_1, v'_2)|\) By definition of \(|\cdot|\)

\(\Gamma \vdash \text{M} e' : (F(\text{Ref}[M(X)]A)) \triangleright (M(X); \emptyset)\) and \(|e| = e'\) where \(e' = \text{ref}(v'_1, v'_2)\) and \(e = \text{ref}(v_1, v_2)\)

- Case \(\Gamma \vdash v \Rightarrow (\text{Nm} \text{Nm} N') \quad \Gamma \vdash N \circ N' e_1 \iff C \triangleright (W; R)\) echk-scop

\(\Gamma \vdash v' : \text{Nm} \text{Nm} \text{Nm} N' \text{ and } |N'| = v'\) By inductive hypothesis

\(\Gamma \vdash N \circ N' e'_1 : C \triangleright (W; R) \text{ and } |e_1| = e'_1\) By inductive hypothesis

\(\Gamma \vdash N \circ \text{scope}(v', e'_1) : C \triangleright (W; R)\) By rule scope

\(|\text{scope}(v, e_1)| = |\text{scope}(|v|, |e_1|)| = |\text{scope}(v', e'_1)|\) By definition of \(|\cdot|; |v| = v'; |e'_1| = e_1\)

\(\Gamma \vdash \text{M} e' : C \triangleright (W; R) \text{ and } |e| = e' \text{ where } e' = \text{scope}(v', e'_1)\) and \(e = \text{scope}(v, e_1)\)

- Case \(\Gamma, \alpha : \gamma \vdash M t \iff E\) echk-\(\forall\)IndexIntro

\(\Gamma, \alpha : \gamma \vdash M t' : E \text{ and } |t| = t'\) By inductive hypothesis

\(\Gamma \vdash M t' : (\forall \alpha : \gamma. E)\) By rule AllIntro

\(\Gamma \vdash \text{M} e' : (\forall \alpha : \gamma. E) \text{ and } |e| = e' \text{ where } e' = t'\) and \(e = t\)

- Case \(\Gamma, \alpha : \gamma \vdash M t \iff E\) echk-\(\forall\)Intro

\(\exists t' \text{ such that } \Gamma, \alpha : \gamma \vdash M t' : E \text{ and } |t| = t'\) By inductive hypothesis

\(\Gamma \vdash M t' : (\forall \alpha : K. E)\) By rule AllIntro

\(\Gamma \vdash \text{M} e' : (\forall \alpha : K. E) \text{ and } |e| = e' \text{ where } e' = t'\) and \(e = t\)

- Case \(\Gamma \vdash M e \Rightarrow E_1 \quad E_1 = E_2\) echk-sub

By i.h. and etype-sub. \(\Box\)
Theorem D.4 (Completeness of Bidirectional Computation Typing). If $\Gamma \vdash^M e : E$, then there exist computations $e', e''$ such that

1. $\Gamma \vdash^M e' \Rightarrow E$ and $|e'| = e$
2. $\Gamma \vdash^M e'' \Leftarrow E$ and $|e''| = e$

Proof. By induction on the derivation of $\Gamma \vdash^M e : E$.

- **Case** etype-sub: By i.h. and echk-sub.

- **Case** $\Gamma \vdash v : (A_1 \times A_2)$
  
  $\Gamma, x_1 : A_1, x_2 : A_2 \vdash^M e_1 : E$
  
  $\Gamma \vdash^M \text{split}(v, x_1, x_2, e_1) : E$
  
  $\Gamma, x_1 : A_1, x_2 : A_2 \vdash e'_1 \Leftarrow E$ and $e_1 = |e'_1|$ 
  
  By inductive hypothesis
  
  $\Gamma \vdash v' \Rightarrow (A_1 \times A_2)$ and $v_1 = |v'_1|$ 
  
  By Thm. D.2
  
  $\Gamma \vdash^M \text{split}(v', x_1, x_2, e'_1) \Leftarrow E$ 
  
  By chk-split
  
  $\Gamma \vdash^M (\text{split}(v', x_1, x_2, e'_1) : E) \Rightarrow E$ 
  
  By syn-anno
  
  $\text{split}(v', x_1, x_2, e'_1) = \text{split}(v, x_1, x_2, e_1)$ 
  
  Since $|v'| = v, |e'_1| = e_1$

- **Case** $\Gamma \vdash e' \Rightarrow E$ and $|e'| = e$
  
  where $e' = \text{split}(v', x_1, x_2, e'_1)$
  
  and $e = \text{split}(v, x_1, x_2, e_1)$

- **Case** $\Gamma \vdash e'' \Leftarrow E$ and $|e''| = e$
  
  where $e'' = (\text{split}(v', x_1, x_2, e'_1) : E)$
  
  and $e = \text{split}(v, x_1, x_2, e_1)$

- **Case** $\Gamma \vdash v : (A_1 + A_2)$
  
  $\Gamma, x_1 : A_1 \vdash^M e_1 : E$
  
  $\Gamma, x_2 : A_2 \vdash^M e_2 : E$
  
  $\Gamma \vdash^M \text{case}(v, x_1, e_1, x_2, e_2) : E$
  
  $\Gamma \vdash v' \Rightarrow (A_1 + A_2)$ and $|v'| = v$ 
  
  By Thm. D.2
  
  $\Gamma, x_1 : A_1 \vdash^M e''_1 \Leftarrow E$ and $|e''_1| = e_1$ 
  
  By inductive hypothesis
  
  $\Gamma, x_2 : A_2 \vdash^M e''_2 \Leftarrow E$ and $|e''_2| = |e_2|$ 
  
  By inductive hypothesis
  
  $\Gamma \vdash^M \text{case}(v', x_1, e''_1, x_2, e''_2) \Leftarrow E$ 
  
  By rule chk-case
  
  $\Gamma \vdash^M (\text{case}(v', x_1, e''_1, x_2, e''_2) : E) \Rightarrow E$ 
  
  By rule chk-conv
  
  $\text{case}(v', x_1, e''_1, x_2, e''_2) = \text{case}(v, x_1, e_1, x_2, e_2)$

- **Case** $\Gamma \vdash e' \Rightarrow E$ and $|e'| = e$
  
  where $e' = \text{case}(v', x_1, e''_1, x_2, e''_2) : E$ 
  
  and $e = \text{case}(v, x_1, e_1, x_2, e_2)$

- **Case** $\Gamma \vdash e'' \Leftarrow E$ and $|e''| = e$
  
  where $e'' = \text{case}(v', x_1, e''_1, x_2, e''_2)$
  
  and $e = \text{case}(v, x_1, e_1, x_2, e_2)$

- **Case** $\Gamma \vdash v : A$
  
  $\Gamma \vdash^M \text{ret}(v) : (\langle F A \rangle \triangleright \langle 0; 0 \rangle)$
Let $E = (\{FA\} \triangleright \langle \emptyset; \emptyset \rangle)$

\[
\exists \nu'' \text{ such that } \Gamma \vdash \nu'' \triangleleft A \text{ and } |\nu''| = v
\]

By Thm. D.2

\[
\begin{align*}
\Gamma \vdash M \quad \text{ret}($$\nu'')$$ \triangleleft E & \\
\Gamma \vdash M \quad (\text{ret}($$\nu'') : E) \Rightarrow E & \\
\end{align*}
\]

By rule chk-ret

By syn-anno

By definition of $|$-$|

and $|\nu''| = v$

\[
\begin{align*}
\Gamma \vdash M e' & \Rightarrow E \text{ and } |e'| = e \\
& \text{ where } e' = (\text{ret}($$\nu'') : E) \text{ and } e = \text{ret}($$\nu)
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash M e'' & \Rightarrow E \text{ and } |e''| = e \\
& \text{ where } e'' = \text{ret}($$\nu'') \text{ and } e = \text{ret}($$\nu)
\end{align*}
\]

\[\text{Case}\]

\[
\begin{align*}
\Gamma \vdash M e_1 : (FA) \triangleright e_1 & \quad \Gamma, x : A \vdash M e_2 : (C \triangleright e_2) & \\
\Gamma \vdash M \text{let}(e_1, x.e_2) : (C \triangleright (e_1 \text{ then } e_2)) & \text{let}
\end{align*}
\]

Let $E = (C \triangleright (e_1 \text{ then } e_2))$

\[
\begin{align*}
\Gamma \vdash M e_1' \Rightarrow (FA) \triangleright e_1 & \quad \text{By inductive hypothesis} \\
\Gamma, x : A \vdash M e_2'' \triangleleft (C \triangleright e_2) & \quad \text{By inductive hypothesis} \\
\Gamma \vdash M \text{let}(e_1', x.e_2'') \triangleleft E & \\
\Gamma \vdash M \text{let}(e_1', x.e_2'') : (C \triangleright e_2) & \text{By rule chk-let}
\end{align*}
\]

By rule chk-conv

By definition of $|$-$|

and $|e_1'| = e_1$, $|e_2''| = e_2$

\[
\begin{align*}
\Gamma \vdash M e' & \Rightarrow E \text{ and } |e'| = e \quad \text{ where } e' = (\text{let}(e_1', x.e_2'') : E) \text{ and } e = \text{let}(e_1, x.e_2) \\
\Gamma \vdash M e'' & \Rightarrow E \text{ and } |e''| = e \quad \text{ where } e'' = \text{let}(e_1', x.e_2'') \text{ and } e = \text{let}(e_1, x.e_2)
\end{align*}
\]

\[\text{Case}\]

\[
\begin{align*}
\Gamma, x : A \vdash M e_1 : E_1 & \\
\Gamma \vdash M (\lambda x. e_1) : ((A \rightarrow E_1) \triangleright \langle \emptyset; \emptyset \rangle) & \text{lam}
\end{align*}
\]

Let $E = ((A \rightarrow E_1) \triangleright \langle \emptyset; \emptyset \rangle)$

\[
\begin{align*}
\exists e_1'' \text{ such that } \Gamma, x : A \vdash M e_1'' \triangleleft E_1 \text{ and } |e_1''| = e_1 & \\
\Gamma \vdash M \lambda x. e_1'' \triangleleft E_1 & \\
\Gamma \vdash M ((\lambda x. e_1'') : E_1) \Rightarrow E & \text{By syn-anno}
\end{align*}
\]

By definition of $|$-$|

and $|e_1''| = e_1$

\[
\begin{align*}
\Gamma \vdash M e' & \Rightarrow E \text{ and } |e'| = e \quad \text{ where } e' = ((\lambda x. e_1'') : E) \text{ and } e = (\lambda x. e_1) \\
\Gamma \vdash M e'' & \Rightarrow E \text{ and } |e''| = e \quad \text{ where } e'' = (\lambda x. e_1'') \text{ and } e = (\lambda x. e_1)
\end{align*}
\]

\[\text{Case}\]

\[
\begin{align*}
\Gamma \vdash M e_1 : ((A \rightarrow E) \triangleright e_1) & \\
\Gamma \vdash v : A &
\end{align*}
\]

\[
\begin{align*}
\exists e_1' \text{ such that } \Gamma \vdash M e_1' \Rightarrow ((A \rightarrow E) \triangleright e_1) \text{ and } |e_1'| = e_1 & \\
\exists v'' \text{ such that } \Gamma \vdash v'' \triangleleft A \text{ and } |v''| = v & \\
\Gamma \vdash M (e_1' \quad v'') \Rightarrow (E \text{ after } e_1) & \\
\Gamma \vdash M (e_1' \quad v'') \triangleleft (E \text{ after } e_1) & \text{By rule chk-conv}
\end{align*}
\]

By the definition of $|$-$|

and $|e_1'| = e_1$, $|v''| = v$
Fungi: Typed incremental computation with names

\[
\begin{align*}
\text{Case} & \quad \Gamma \vdash v : \text{Nm}[X] \quad \Gamma \vdash M e_1 : E \\
\frac{}{\Gamma \vdash \text{thunk}(v, e_1) : (F(\text{Thk}[M(X)] E)) \triangleright \langle M(X); \emptyset \rangle}
\end{align*}
\]

Let \( E = (F(\text{Thk}[M(X)] E)) \triangleright \langle M(X); \emptyset \rangle \)

\[
\begin{align*}
\exists v'' \text{ such that } \Gamma \vdash v'' & \iff \text{Nm}[X] \text{ and } |v''| = v \\
\exists e_1' \text{ such that } \Gamma \vdash M e_1' & \iff E \text{ and } |e_1'| = e_1 \\
\Gamma \vdash M \text{thunk}(v'', e_1') & \iff E \\
\Gamma \vdash M (\text{thunk}(v'', e_1') : E) \triangleright E & \iff \text{rule syn-anno} \\
|\text{thunk}(v'', e_1')| = \text{thunk}(v'', e_1') & \iff |\text{thunk}(v'', |v''|)| = \text{thunk}(v, e_1) \\
\text{By definition of } |\cdot| \\
& \iff |v''| = v, |e_1'| = e_1
\end{align*}
\]

\[
\begin{align*}
\text{Case} & \quad \Gamma \vdash v : \text{Thk}[X] (C \triangleright e) \\
\frac{}{\Gamma \vdash \text{force}(v) : (C \triangleright (\emptyset; X \text{ then } e))}
\end{align*}
\]

Let \( E = (C \triangleright (\emptyset; X \text{ then } e)) \)

\[
\begin{align*}
\Gamma \vdash v' & \iff \text{Thk}[X] (C \triangleright e) \text{ and } |v'| = v \\
\Gamma \vdash M \text{force}(v') & \iff E \\
\Gamma \vdash M \text{force}(v') & \iff E \\
|\text{force}(v')| = |\text{force}(v')| = |\text{force}(v)| & \iff |\text{definition of } |\cdot|| \\
& \iff |v'| = v
\end{align*}
\]

\[
\begin{align*}
\text{Case} & \quad \Gamma \vdash v_1 : \text{Nm}[X] \quad \Gamma \vdash v_2 : A \\
\frac{}{\Gamma \vdash \text{ref}(v_1, v_2) : (F(\text{Ref}[M(X)] A)) \triangleright \langle M(X); \emptyset \rangle}
\end{align*}
\]

Let \( E = (F(\text{Ref}[M(X)] A)) \triangleright \langle M(X); \emptyset \rangle \)

\[
\begin{align*}
\Gamma \vdash v_1' & \iff \text{Nm}[X] \text{ and } |v_1'| = v_1 \\
\Gamma \vdash v_2' & \iff A \text{ and } |v_2'| = v_2 \\
\Gamma \vdash M \text{ref}(v_1', v_2') & \iff E \\
\Gamma \vdash M (\text{ref}(v_1', v_2') : E) \triangleright E & \iff \text{rule syn-anno} \\
|\text{ref}(v_1', v_2')| = |\text{ref}(v_1', v_2')| & \iff |\text{ref}(v_1', |v_1'|)| = \text{ref}(v_1, v_2) \\
& \iff |v_1'| = v_1, |v_2'| = v_2
\end{align*}
\]
• Case
\[ \Gamma \vdash v : \text{Ref}[X] \ A \]
\[ \Gamma \vdash \text{get}(v) : (\text{F} A) \triangleright \langle \emptyset ; X \rangle \]
- \[ \Gamma \vdash v' \Rightarrow \text{Ref}[X] \ A \text{ and } |v'| = v \] By Thm. D.2
- \[ \Gamma \vdash \text{get}(v') \Rightarrow (\text{F} A) \triangleright \langle \emptyset ; X \rangle \] By rule syn-get
- \[ \Gamma \vdash \text{get}(v') \triangleleft (\text{F} A) \triangleright \langle \emptyset ; X \rangle \] By rule chk-conv
- \[ |\text{get}(v')| = |\text{get}(v')| = \text{get}(v) \] By definition of |−|
  and \[ |v'| = v \]
- \[ \Rightarrow \Gamma \vdash M e' \Rightarrow (\text{F} A) \triangleright \langle \emptyset ; X \rangle \text{ and } |e'| = e \] where \( e' = \text{get}(v') \) and \( e = \text{get}(v) \)
- \[ \Rightarrow \Gamma \vdash M e'' \triangleleft (\text{F} A) \triangleright \langle \emptyset ; X \rangle \text{ and } |e''| = e \] where \( e'' = \text{get}(v') \) and \( e = \text{get}(v) \)

• Case
\[ \Gamma \vdash v_M : (\text{Nm} \triangleright\triangleright \text{Nm})[M] \]
\[ \Gamma \vdash v : \text{Nm}[i] \]
\[ \Gamma \vdash N (v_M v) : F (\text{Nm}[M(i)]) \triangleright \langle \emptyset ; \emptyset \rangle \] name-app
- \[ \Rightarrow \Gamma \vdash v_M' \Rightarrow (\text{Nm} \triangleright\triangleright \text{Nm})[M] \text{ and } |v_M'| = v_M \] By Thm. D.2
- \[ \Rightarrow \Gamma \vdash v' \Rightarrow \text{Nm}[i] \text{ and } |v'| = v \] By Thm. D.2
- \[ \Rightarrow \Gamma \vdash N (v_M' v') \Rightarrow F (\text{Nm}[M(i)]) \triangleright \langle \emptyset ; \emptyset \rangle \] By rule syn-name-app
- \[ \Rightarrow \Gamma \vdash N (v_M' v') \triangleleft F (\text{Nm}[M(i)]) \triangleright \langle \emptyset ; \emptyset \rangle \] By rule chk-conv
- \[ |(v_M' v')| = |(v_M' | v')| = (v_M v) \] By definition of |−|
  and \[ |v_M'| = v_M, |v'| = v \]
- \[ \Rightarrow \Gamma \vdash N e' \Rightarrow F (\text{Nm}[M(i)]) \triangleright \langle \emptyset ; \emptyset \rangle \text{ and } |e'| = e \] where \( e' = (v_M' v') \) and \( e = (v_M v) \)
- \[ \Rightarrow \Gamma \vdash N e'' \triangleleft F (\text{Nm}[M(i)]) \triangleright \langle \emptyset ; \emptyset \rangle \text{ and } |e''| = e \] where \( e'' = (v_M' v') \) and \( e = (v_M v) \)

• Case
\[ \Gamma \vdash v : (\text{Nm} \triangleright\triangleright \text{Nm})[N'] \]
\[ \Gamma \vdash N^\triangleright N' e_1 : C \triangleright \langle W ; R \rangle \]
\[ \Gamma \vdash N \text{scope}(v, e_1) : C \triangleright \langle W ; R \rangle \] scope
- \[ \text{Let } E = C \triangleright \langle W ; R \rangle \]
- \[ \exists v'' \text{ such that } \Gamma \vdash v'' \Rightarrow (\text{Nm} \triangleright\triangleright \text{Nm})[N'] \text{ and } |v''| = v \] By Thm. D.2
- \[ \exists e'_1 \text{ such that } \Gamma \vdash N^\triangleright N' e'_1 \triangleleft E \text{ and } |e'_1| = e_1 \]
- \[ \text{By inductive hypothesis} \]
- \[ \Gamma \vdash N \text{scope}(v'', e'_1) \triangleleft E \] By rule chk-scope
- \[ \Gamma \vdash N (\text{scope}(v'', e'_1) : E) \triangleright E \] By rule syn-anno
- \[ |(\text{scope}(v'', e'_1) : E)| = |(\text{scope}(v'', e'_1)| \] By definition of |−|
- \[ |(\text{scope}(v'', e'_1)| = |(\text{scope}(v'', e'_1)| = \text{scope}(v, e_1) \] By definition of |−|
- \[ \Rightarrow \Gamma \vdash M e' \Rightarrow E \text{ and } |e'| = e \] where \( e' = (\text{scope}(v'', e'_1) : E) \) and \( e = \text{scope}(v, e_1) \)
- \[ \Rightarrow \Gamma \vdash M e'' \triangleleft E \text{ and } |e''| = e \] where \( e'' = \text{scope}(v'', e'_1) \) and \( e = \text{scope}(v, e_1) \)

• Case
\[ \Gamma, a : \gamma \vdash M t : E \]
\[ \Gamma \vdash M t : (\forall a : \gamma, E) \] etype-\gamma IndexIntro

Matthew A. Hammer, Jana Dunfield, Kyle Headley, Monal Narasimhamurthy, and Dimitrios J. Economou.

: Vol. 1, No. 1, Article . Publication date: May 2021.
∃ t’’ such that Γ; a : γ ⊢ M t’’ ⇐ E and |t’’| = t
By inductive hypothesis
Γ ⊢ (∀a : γ. E)
By rule chk-AllIndexIntro
Γ ⊢ (t’’ : (∀a : γ. E)) ⇒ (∀a : γ. E)
By rule syn-anno
| (t’’ : (∀a : γ. E)) | = | t’’ | = t
By definition of |−| and |t’’| = t

∃ e’ such that Γ ⊢ M e’ ⇒ (∀a : γ. E) and |e’| = e
where e’ = (t’’ : (∀a : γ. E)) and e = t
Γ ⊢ i : γ
Given
Γ ⊢ M e’ ⇒ [i/a]E
By rule syn-AllIndexElim
Γ ⊢ M e’ ⇐ [i/a]E
By rule chk-conv

• Case
Γ ⊢ M e : (∀a : γ. E)  Γ ⊢ i : γ
Γ ⊢ M e : [i/a]E
etype-∀IndexElim

∃ e’ such that Γ ⊢ M e’ ⇒ (∀a : γ. E) and |e’| = e
By inductive hypothesis
Γ ⊢ i : γ
Given
Γ ⊢ M e’ ⇒ [i/a]E
By rule syn-AllIndexElim
Γ ⊢ M e’ ⇐ [i/a]E
By rule chk-conv

• Case
Γ ⊢ M e’ [i] ⇒ [i/a]E and |e’[i]| = e
where e’ = t’’ and e = t

E NAME TERM LANGUAGE

We define a restricted name term language for computing larger names from smaller names. This language consists of the following:

• Syntax for names, name terms and sorts (Fig. 8 in Sec. 3.2).
• Name term sorting: A judgment that assigns sorts to name terms (Fig. 9 in Sec. 3.2).
• Big-step evaluation for name terms: A judgment that assigns name term values to name terms (Fig. 9 in Sec. 3.2).
• Semantic definition of equivalent and disjoint name terms (Sec. E.1).
• Logical proof rules for equivalent and disjoint name terms: Two judgements that should be sound with respect to the semantic definitions of equivalence and disjointness (Fig. 24 and Fig. 25).

The first three items are each described in Sec. 3.2. We define the last two items in this section.

E.1 Semantic equivalence and disjointness

Below, we define semantic equivalence and disjointness of (sorted) name terms. We define these semantic properties inductively, based on the common sort of the name terms. In this sense, these definitions can be viewed as instances of logical relations.
We define contexts \( \Gamma \) that relate two variables; each declaration either asserts that \( a \) and \( b \) are equivalent, or disjoint. We write \( \Gamma.1 \) and \( \Gamma.2 \) for the projection of a relational \( \Gamma \) into an ordinary \( \Gamma \) suitable for the left-hand (\( \Gamma.1 \)) or right-hand (\( \Gamma.2 \)) sides. Also, we write \( \text{flip}(\Gamma) \) for the operation of exchanging \( a \) and \( b \) in each declaration: \( \text{flip}( (a \perp b : \gamma)) = (b \perp a : \gamma) \), so that \( \text{flip}(\Gamma).1 = \Gamma.2 \) and \( \text{flip}(\Gamma).2 = \Gamma.1 \).

**Definition E.1** (Closing substitutions).
We define closing substitution pairs related by equivalence and disjointness assumptions in a context \( \Gamma \). These definitions use and are used by the definitions below for equivalence and apartness of open terms.

- \( \vdash \sigma_1 \equiv \sigma_2 : \Gamma \) means that \( (x \equiv y : \gamma) \in \Gamma \) implies \( (\sigma_1(x) = N \text{ and } \sigma_2(y) = M \text{ and } \vdash N \equiv M : \gamma) \)
- \( \vdash \sigma_1 \perp \sigma_2 : \Gamma \) means that \( (x \perp y : \gamma) \in \Gamma \) implies \( (\sigma_1(x) = N \text{ and } \sigma_2(y) = M \text{ and } \vdash N \perp M : \gamma) \)
- \( \vdash \sigma_1 \sim \sigma_2 : \Gamma \) means that \( \vdash \sigma_1 \equiv \sigma_2 : \Gamma \text{ and } \vdash \sigma_1 \perp \sigma_2 : \Gamma \)

**Definition E.2** (Semantic equivalence). We define \( \Gamma \vdash M_1 \equiv M_2 : \gamma \) as follows:

\( \Gamma.1 \vdash M_1 : \gamma \text{ and } (\Gamma).2 \vdash M_2 : \gamma \text{ and, for all } \sigma_1, \sigma_2 \text{ such that } \vdash \sigma_1 \equiv \sigma_2 : \Gamma \text{ and } [\sigma_1]M_1 \downarrow V_1 \text{ and } [\sigma_2]M_2 \downarrow V_2, \text{ we have the following about } V_1 \text{ and } V_2: \)

<table>
<thead>
<tr>
<th>Sort (( \gamma ))</th>
<th>Values ( V_1 ) and ( V_2 ) of sort ( \gamma ) are equivalent, written ( \vdash V_1 \equiv V_2 : \gamma )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Always</td>
</tr>
<tr>
<td>Nm</td>
<td>When ( V_1 = n_1 ) and ( V_2 = n_2 ) and ( n_1 = n_2 ) (identical binary trees)</td>
</tr>
</tbody>
</table>
| \( \gamma_1 \neq \gamma_2 \) | When \( V_1 = (\langle V_{11}, V_{12} \rangle) \) and \( V_1 = (V_{21}, V_{22}) \)  
|                   | and \( \vdash V_{11} \equiv V_{21} : \gamma_1 \text{ and } \vdash V_{21} \equiv V_{22} : \gamma_2 \) |
| \( \gamma_1 \rightarrow \gamma_2 \) | When \( V_1 = \lambda a_1.M_1 \) and \( V_2 = \lambda a_2.M_2, \)  
|                   | and for all name terms \( \vdash N_1 \equiv N_2 : \gamma_1, \)  
|                   | \( [N_1/a_1]M_1 \downarrow W_1 \text{ and } [N_2/a_2]M_2 \downarrow W_2 \text{ implies } \vdash W_1 \equiv W_2 : \gamma_2 \) |

**Definition E.3** (Semantic apartness). We define \( \Gamma \vdash M_1 \perp M_2 : \gamma \) as follows:

\( \Gamma.1 \vdash M_1 : \gamma \text{ and } (\Gamma).2 \vdash M_2 : \gamma \text{ and, for all } \sigma_1, \sigma_2 \text{ such that } \vdash \sigma_1 \sim \sigma_2 : \Gamma \text{ and } [\sigma_1]M_1 \downarrow V_1 \text{ and } [\sigma_2]M_2 \downarrow V_2, \text{ we have the following about } V_1 \text{ and } V_2: \)

\( \vdash \)
\[ \Gamma \vdash M \equiv N : \gamma \] The name terms \( M \) and \( N \) are equivalent at sort \( \gamma \)

\[
\begin{align*}
(M \equiv N : \gamma) & \in \Gamma & \text{Eq-Var} \\
\Gamma \vdash M \equiv N : \gamma & \text{E-Ref} \\
\Gamma \vdash M \equiv M : \gamma & \text{E-Sym} \\
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash M_1 \equiv M_2 : \gamma & \text{Eq-Trans} \\
\Gamma \vdash M_3 \equiv M_2 : \gamma & \\
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash M_1 \equiv N_1 : \gamma_1 & \quad \Gamma \vdash M_2 \equiv N_2 : \gamma_2 & \text{Eq-Pair} \\
\Gamma \vdash (M_1, M_2) \equiv (N_1, N_2) : \gamma_1 * \gamma_2 & \\
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash M_1 \equiv N_1 : \text{Nm} & \quad \Gamma \vdash M_2 \equiv N_2 : \text{Nm} & \text{Eq-Bin} \\
\end{align*}
\]

\[
\begin{align*}
\Gamma, (a \equiv b : \gamma_1) \vdash M \equiv N : \gamma_2 & \quad \Gamma \vdash M_1 \equiv N_1 : \gamma_1 \text{Nm} \gamma_2 & \text{Eq-Lam} \\
\Gamma \vdash \lambda a. M \equiv \lambda b. N : \gamma_1 \text{Nm} \gamma_2 & \quad \Gamma \vdash M_2 \equiv N_2 : \gamma_1 & \\
\Gamma, \alpha \equiv a : \gamma_1 \vdash M_1 \equiv M'_1 : \gamma_2 & \quad \Gamma \vdash \lambda a. M_1 M_2 \equiv [M'_2 / a]M'_1 : \gamma_2 & \text{Eq-\beta} \\
\end{align*}
\]

Fig. 24. Deductive rules for showing that two name terms are equivalent

<table>
<thead>
<tr>
<th>Sort (( \gamma ))</th>
<th>Values ( V_1 ) and ( V_2 ) of sort ( \gamma ) are apart, written ( \parallel V_1 \land V_2 : \gamma )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Always</td>
</tr>
<tr>
<td>Nm</td>
<td>When ( V_1 = n_1 ) and ( V_2 = n_2 ) and ( n_1 \neq n_2 ) (distinct binary trees)</td>
</tr>
<tr>
<td>( \gamma_1 \ast \gamma_2 )</td>
<td>When ( V_1 = (V_{11}, V_{12}) ) and ( V_1 = (V_{21}, V_{22}) ) and ( \parallel V_{11} \land V_{21} : \gamma_1 ) and ( \parallel V_{21} \land V_{22} : \gamma_2 )</td>
</tr>
<tr>
<td>( \gamma_1 ) \text{Nm} ( \gamma_2 )</td>
<td>When ( V_1 = \lambda a_1. M_1 ) and ( V_2 = \lambda a_2. M_2 ) and for all name terms ( \vdash N_1 : \gamma_1 ) and ( \vdash N_2 : \gamma_1 ), ( [N_1 / a_1]M_1 \parallel W_1 ) and ( [N_2 / a_2]M_2 \parallel W_2 ) implies ( \parallel W_1 \land W_2 : \gamma_2 )</td>
</tr>
</tbody>
</table>

E.2 Metatheory of name term language

Some lemmas in this section are missing complete proofs and should be considered conjectures (Lemma E.1 (Projections of syntactic equivalence)–Lemma E.8 (Reflexivity of name term evaluation)).

**Lemma E.1 (Projections of syntactic equivalence).**

If \( \Gamma \vdash M_1 \equiv M_2 : \gamma \), then \( \Gamma.1 \vdash M_1 : \gamma \) and \( \Gamma.2 \vdash M_2 : \gamma \).

**Lemma E.2 (Determinism of evaluation up to substitution).**

If \( \Gamma.1 \vdash M : \gamma \) and \( \Gamma.2 \vdash M : \gamma \) and \( \parallel \sigma_1 \equiv \sigma_2 : \Gamma \) and \( [\sigma_1]M \parallel V_1 \) and \( [\sigma_2]M \parallel V_2 \) then there exists \( V \) such that \( V_1 = [\sigma_1]V \) and \( V_2 = [\sigma_2]V \).

**Lemma E.3 (Reflexivity of semantic equivalence).**

(1) If \( \vdash M : \gamma \) then \( \parallel M \equiv M : \gamma \).

(2) If \( \Gamma.1 \vdash V : \gamma \) and \( \Gamma.2 \vdash V : \gamma \) and \( \parallel \sigma_1 \equiv \sigma_2 : \Gamma \) and \( V_1 = [\sigma_1]V \) and \( V_2 = [\sigma_2]V \) then \( \parallel V_1 \equiv V_2 : \gamma \).
The name terms $M$ and $N$ are apart at sort $\gamma$

\[
\frac{(a \perp b : \gamma) \in \Gamma}{\Gamma \vdash a \perp b : \gamma} \quad \text{Var} \\
\frac{\text{flip}(\Gamma) \vdash N \perp M : \gamma}{\Gamma \vdash M \perp N : \gamma} \quad \text{D-Sym}
\]

\[
\frac{\Gamma \vdash M_1 \equiv M_2 : \gamma}{\Gamma \vdash M_1 \perp M_2 : \gamma} \quad \text{D-trans}
\]

\[
\frac{\Gamma \vdash M_1 \perp N_1 : Nm}{\Gamma \vdash \langle\langle M_1, M_2\rangle\rangle \perp \langle\langle N_1, N_2\rangle\rangle : Nm} \quad \text{D-Bin}_1
\]

\[
\frac{\Gamma \vdash M_1 \equiv M_2 : Nm}{\Gamma \vdash \langle\langle M_2, M\rangle\rangle \perp \langle\langle N_1, N\rangle\rangle : Nm} \quad \text{D-Bin}_2
\]

\[
\frac{\Gamma \vdash M \perp N : \gamma}{\Gamma \vdash \lambda a. M \perp \lambda b. N : \gamma} \quad \text{D-Lam}
\]

\[
\frac{\Gamma, a : \gamma \vdash M_1 : \gamma}{\Gamma \vdash (\lambda a. M_1) M_2 \perp N : \gamma} \quad \text{D-\beta}
\]

Fig. 25. Deductive rules for showing that two name terms are apart.

**Lemma E.4 (Type Safety).** If $\Gamma \vdash M : \gamma$ and $[\sigma]M \Downarrow [\sigma]V$ then $\Gamma \vdash V : \gamma$.

**Lemma E.5 (Symmetry of Semantic Equivalence).**

1. If $\models \sigma_1 \equiv \sigma_2 : \Gamma$ then $\models \sigma_2 \equiv \sigma_1 : \text{flip}(\Gamma)$.
2. If $\models V_1 \equiv V_2 : \gamma$ then $\models V_2 \equiv V_1 : \gamma$.
3. If $\models M_1 \equiv M_2 : \gamma$ then $\models M_2 \equiv M_1 : \gamma$.
4. If $\models M_1 \equiv M_2 : \gamma$ then $\models \text{flip}(\Gamma) \models M_2 \equiv M_1 : \gamma$.

**Lemma E.6 (Evaluation Respects Semantic Equivalence).**

If $\Gamma \models M \equiv N : \gamma$ and $\models \sigma_1 \equiv \sigma_2 : \Gamma$ and $[\sigma_1]M \Downarrow V_1$ then there exists $V_2$ such that $[\sigma_2]N \Downarrow V_2$ and $\models V_1 \Downarrow V_2 : \gamma$.

**Lemma E.7 (Closing Substitutions Respect Syntactic Equivalence).**

If $\models \sigma_1 \equiv \sigma_2 : \Gamma$ and $\Gamma \models M_1 \equiv M_2 : \gamma$ then $\models [\sigma_1]M_1 \equiv [\sigma_2]M_2 : \gamma$.

**Lemma E.8 (Reflexivity of Name Term Evaluation).**

If $\Gamma, a : \gamma \vdash M_1 : \gamma$ and $\Gamma, a : \gamma \vdash M_2 : \gamma$ and $\models \sigma_1 \equiv \sigma_2 : \Gamma$ and $[\sigma_1]M \Downarrow V_1$ and $[\sigma_2]M \Downarrow V_2$ then $\models V_1 \Downarrow V_2 : \gamma$.

**Lemma E.9 (Transitivity of Value Equivalence).**

If $\Gamma \vdash V_1 : \gamma$ and $\models V_1 \equiv V_2 : \gamma$ and $\models V_2 \equiv V_3 : \gamma$ then $\models V_1 \equiv V_3 : \gamma$.

**Proof.** Uses strong normalization. $\square$

**Conjecture E.10 (Soundness of Deductive Equivalence).**

If $\Gamma \vdash M_1 \equiv M_2 : \gamma$ then $\Gamma \models M_1 \equiv M_2 : \gamma$.

**Proof.** By induction on the given derivation.
Case \( (a \equiv b : \gamma) \in \Gamma \)
\[
\Gamma \vdash a \equiv b : \gamma
\]

By definition of closing substitutions.

Case \( \Gamma, 1 \vdash M : \gamma \quad \Gamma, 2 \vdash M : \gamma \)
\[
\Gamma \vdash M \equiv M : \gamma
\]

Eq-Refl

By Lemma E.2 (Determinism of evaluation up to substitution), Lemma E.4 (Type safety), and Lemma E.3 (Reflexivity of semantic equivalence).

Case \( \Gamma \vdash N \equiv M : \gamma \)
\[
\Gamma \vdash M \equiv N : \gamma
\]

Eq-Sym

By Lemma E.5 (Symmetry of semantic equivalence).

Case \( \Gamma \vdash M_1 \equiv M_2 : \gamma \quad \Gamma \vdash M_2 \equiv M_3 : \gamma \)
\[
\Gamma \vdash M_1 \equiv M_3 : \gamma
\]

Eq-Trans

By idempotency of flipping relational contexts, Lemma E.6 (Evaluation respects semantic equivalence), inductive hypotheses on the two given subderivations, Lemma E.5 (Symmetry of semantic equivalence), and Lemma E.9 (Transitivity of value equivalence).

Case \( \Gamma \vdash M_1 \equiv N_1 : \gamma_1 \quad \Gamma \vdash M_2 \equiv N_2 : \gamma_2 \)
\[
\Gamma \vdash (M_1, M_2) \equiv (N_1, N_2) : \gamma_1 \ast \gamma_2
\]

Eq-Pair

By the definition of substitution and the i.h.

Case \( \Gamma \vdash M_1 \equiv N_1 : \text{Nm} \quad \Gamma \vdash M_2 \equiv N_2 : \text{Nm} \)
\[
\Gamma \vdash \langle M_1, M_2 \rangle \equiv \langle N_1, N_2 \rangle : \text{Nm}
\]

Eq-Bin

By the definition of substitution and the i.h.

Case \( \Gamma, (a \equiv b : \gamma_1) \vdash M \equiv N : \gamma_2 \)
\[
\Gamma \vdash \lambda a. M \equiv \lambda b. N : \gamma_1 \overset{\text{Nm}}{\Rightarrow} \gamma_2
\]

Eq-Lam

By transposition of substitutions and the i.h.

Case \( \Gamma \vdash M_1 \equiv N_1 : \gamma_1 \quad \Gamma \vdash M_2 \equiv N_2 : \gamma_1 \)
\[
\Gamma \vdash M_1(M_2) \equiv N_1(N_2) : \gamma_2
\]

Eq-App

By definition of substitution and inversion (teval-app) of resulting derivations, the inductive hypothesis on the two given syntactic equivalence subderivations (of Eq-App), and definition of semantic equivalence of arrow-sorted values, we get the result.

Case \( \Gamma \vdash M_2 \equiv M'_2 : \gamma_1 \quad \Gamma, a \equiv a : \gamma_1 \vdash M_1 \equiv M'_1 : \gamma_2 \)
\[
\Gamma \vdash (\lambda a. M_1)M_2 \equiv [M'_2/a]M'_1 : \gamma_2
\]

Eq-\(\beta\)

Fix \( \sigma_1 \equiv \sigma_2 : \Gamma \). Suppose \( [\sigma_1](\langle \lambda a. M_1 \rangle M_2) \downarrow V_1 \) and \( [\sigma_2](\langle \lambda a. M'_2 \rangle M'_1) \downarrow V_2 \). We need to show \( \downarrow V_1 = V_2 : \gamma_2 \). By the definition of substitution and inversion of teval-app, \( [\sigma_1]M_2 \downarrow V \) and \( [V/a](\tau M_1) \downarrow V_1 \) for some \( V \). Hence, because \( \Gamma, a \equiv a : \gamma_1 \), we have \( [\sigma_1, V/a]M_1 \downarrow V_1 \).
Rewrite $[\sigma_2]([M_2'/a]/M_1') \Downarrow V_2$ as $[\sigma_2, [\sigma_2]M_2'/a]M_1' \Downarrow V_2$. By Lemma E.7 (Closing substitutions respect syntactic equivalence), $\vdash V \equiv [\sigma_2]M_2' : \gamma_1$. Therefore,

$$\vdash (\sigma_1, V/a) \equiv (\sigma_2, [\sigma_2]M_2'/a) : (\Gamma, a \equiv a : \gamma_1)$$

By the inductive hypothesis on $\Gamma, a \equiv a : \gamma_1 \vdash M_1 \equiv M_1' : \gamma_2$, we get $\vdash V_1 \equiv V_2 : \gamma_2$. \hfill \Box

**Conjecture E.11 (Soundness of deductive disjointness).** If $\Gamma \vdash M_1 \not\equiv M_2 : \gamma$ then $\Gamma \not\vdash M_1 \not\equiv M_2 : \gamma$.

**Conjecture E.12 (Completeness of deductive equivalence).** If $\Gamma \not\vdash M_1 \equiv M_2 : \gamma$ then $\Gamma \not\vdash M_1 \equiv M_2 : \gamma$.

**Conjecture E.13 (Completeness of deductive disjointness).** If $\Gamma \not\vdash M_1 \not\equiv M_2 : \gamma$ then $\Gamma \not\vdash M_1 \not\equiv M_2 : \gamma$. 

, Vol. 1, No. 1, Article . Publication date: May 2021.
Index i reduces to index j

\[
\begin{array}{c}
\text{reduce-proj} \\
\text{reduce-map-empty} \\
\text{M injective} \\
\text{reduce-map-\perp} \\
\text{reduce-kleene-outer} \\
\text{reduce-kleene-inner}
\end{array}
\]

Fig. 26. Reduction rules for indices

F INDEX TERM LANGUAGE

We define a restricted index term language for describing name sets and functions that relate them. This language consists of the following:

- Syntax for index terms, and (additional) sorts (Fig. 10 in Sec. 4.1).
- Index term sorting, which assigns sorts to index terms (Fig. 12 in Sec. 4.1).
- Reduction rules for index terms, deriving the judgment \( i \to_\beta j \) (Fig. 26).
- Semantic definitions of equivalent and disjoint index terms (Sec. F.2).
- Deductive rules for equivalent and disjoint index terms, which should be sound with respect to the semantic definitions of equivalence and disjointness (Fig. 29 and Fig. 30).

The first two items are defined in Sec. 4.1. The remaining items are defined here.

F.1 Index reduction

We write \( i \to_\beta j \) for the one-step head reduction of index i to j, defined in Fig. 26. This is essentially \( \beta \)-reduction for functions, products, and mapping name sets (with map \( M[X] \) distributing over union operators).

Based on one-step head reduction, we define one-step reduction \( i \to_{CC} j \) (reducing anywhere within an index, not only at the head) and multi-step reduction \( i \to_{\cdot} j \):

Definition F.1 (Reduction for indices).

1. Let \( \to_{CC} \) be the congruence closure of \( \to_\beta \).
2. Let \( \to_{\cdot} \) be the reflexive-transitive closure of \( \to_{CC} \).

F.2 Semantic equivalence and apartness of index terms

Definition F.2 (Closing substitutions for index terms).

We define closing substitution pairs related by equivalence and disjointness assumptions in a context \( \Gamma \). These definitions use and are used by the definitions below for equivalence and apartness of open terms.

\[
\begin{align*}
\Gamma \vdash \sigma_1 \equiv \sigma_2 & : \Gamma \iff (x \equiv y : \gamma) \in \Gamma \implies (\sigma_1(x) = i \land \sigma_2(y) = j \land \cdot \vdash i \equiv j : \gamma) \\
\Gamma \vdash \sigma_1 \perp \sigma_2 & : \Gamma \iff (x \perp y : \gamma) \in \Gamma \implies (\sigma_1(x) = i \land \sigma_2(y) = j \land \cdot \vdash i \perp j : \gamma) \\
\Gamma \vdash \sigma_1 \sim \sigma_2 & : \Gamma \iff (\vdash \sigma_1 \equiv \sigma_2 : \Gamma \land \vdash \sigma_1 \perp \sigma_2 : \Gamma)
\end{align*}
\]
Matthew A. Hammer, Jana Dunfield, Kyle Headley, Monal Narasimhamurthy, and Dimitrios J. Economou

\[
\Gamma \vdash M \in X \quad \text{Name term } M \text{ is a member of name set } X, \text{ assuming } X \text{ val}
\]

\[
\frac{\Gamma \vdash (\{M\} \land Y) \equiv X : \text{NmSet}}{\Gamma \vdash M \in X} \quad \text{Membership}_1
\]

\[
\frac{\Gamma \vdash (\{M\} \lor Y) \equiv X : \text{NmSet}}{\Gamma \vdash M \in X} \quad \text{Membership}_2
\]

\[
\Gamma \not\vdash M \in X \quad \text{Name term } M \text{ is not a member of name set } X, \text{ assuming } X \text{ val}
\]

\[
\frac{\Gamma \vdash (\{M\} \land X) \equiv Y : \text{NmSet}}{\Gamma \vdash M \not\in X} \quad \text{NonMembership}
\]

\[
\frac{\Gamma \vdash (\{M\} \lor X) \equiv Y : \text{NmSet}}{\Gamma \vdash M \not\in X} \quad \text{NonMembership}
\]

\[
\Gamma \vdash M \not\in X \quad \text{The name of name term } M \text{ is not a member of name set } X, \text{ assuming } X \text{ val}
\]

\[
\frac{\Gamma \vdash (\{M\} \land X) \equiv Y : \text{NmSet}}{\Gamma \vdash M \not\in X} \quad \text{NonMembership}
\]

Fig. 27. Name term membership

**Definition F.3** (Index normal form). An index \( i \) is in index normal form iff none of the rules reduce-proj, reduce-app, reduce-map{-empty, -single, -\( \bot \), -\( \land \), -\( \lor \)} can be applied (anywhere within \( i \)).

Under this definition, normal forms are not unique: the rules reduce-kleene-inner and reduce-kleene-outer can reduce normal forms. In effect, these are normal forms “modulo Kleene closure”.

**Definition F.4** (Semantic equivalence of index terms). We define \( \Gamma \vdash i_1 \equiv i_2 : \gamma \) as follows:

\[
(\Gamma).1 \vdash i_1 : \gamma \text{ and } (\Gamma).2 \vdash i_2 : \gamma \text{ and, for all } \sigma_1, \sigma_2, \text{ and } j_1 \text{ such that } \vdash \sigma_1 \equiv \sigma_2 : \Gamma \text{ and } [\sigma_1]i_1 \rightarrow j_1 \text{ where } j_1 \text{ is in index normal form, there exists } j_2 \text{ such that } j_2 \text{ is in index normal form and } [\sigma_2]i_2 \rightarrow j_2,
\]

we have the following about \( j_1 \) and \( j_2 \):

<table>
<thead>
<tr>
<th>Sort ( \gamma )</th>
<th>Indices ( j_1 ) and ( j_2 ) of sort ( \gamma ) are equivalent, written ( \vdash j_1 \equiv j_2 : \gamma )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Always</strong></td>
</tr>
<tr>
<td>NmSet</td>
<td>When ( ( \vdash M \in j_1 ) if and only if ( \vdash M \in j_2 ) )</td>
</tr>
<tr>
<td>( \gamma_1 \neq \gamma_2 )</td>
<td>When ( j_1 = (j_{11}, j_{12}) ) and ( j_2 = (j_{21}, j_{22}) ) and ( \vdash j_{11} \equiv j_{21} : \gamma_1 ) and ( \vdash j_{12} \equiv j_{22} : \gamma_2 )</td>
</tr>
<tr>
<td>( \gamma_1 \not\rightarrow \gamma_2 )</td>
<td>When ( j_1 = \lambda \alpha_1.X_1 ) and ( j_2 = \lambda \alpha_2.X_2 ), and for all name terms ( \vdash Y_1 \equiv Y_2 : \gamma_1 ), ( (\lambda \alpha_1.X_1)(Y_1) \rightarrow Z_1 ) and ( (\lambda \alpha_2.X_2)(Y_2) \rightarrow Z_2 ) implies ( \vdash Z_1 \equiv Z_2 : \gamma_2 )</td>
</tr>
</tbody>
</table>

**Definition F.5** (Semantic apartness of index terms). We define \( \Gamma \vdash i_1 \not\equiv i_2 : \gamma \) as follows:

\[
(\Gamma).1 \vdash i_1 : \gamma \text{ and } (\Gamma).2 \vdash i_2 : \gamma \text{ and, for all } \sigma_1, \sigma_2, \text{ and } j_1 \text{ such that } \vdash \sigma_1 \equiv \sigma_2 : \Gamma \text{ and } [\sigma_1]i_1 \rightarrow j_1 \text{ where } j_1 \text{ is in index normal form,}
\]

\[ \vdash \]
there exists $j_2$ such that $j_2$ is in index normal form and $[\sigma_2]_{i_2} \rightarrow j_2$, we have the following about $j_1$ and $j_2$:

<table>
<thead>
<tr>
<th>Sort ($\gamma$)</th>
<th>Index values $j_1$ and $j_2$ of sort $\gamma$ are apart, written $\vdash j_1 \perp j_2 : \gamma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1$ $\text{NmSet}$</td>
<td>Always</td>
</tr>
<tr>
<td>$\gamma_1 \neq \gamma_2$</td>
<td>When $\vdash M \in j_1$ implies $\vdash M \notin j_2$ and $\vdash M \notin j_1$</td>
</tr>
<tr>
<td>$\gamma_1 \overset{\text{ax}}{\rightarrow} \gamma_2$</td>
<td>When $j_1 = (j_{i_1}, j_{i_2})$ and $j_2 = (j_{j_1}, j_{j_2})$ and $\vdash j_{i_1} \perp j_{j_1} : \gamma_1$ and $\vdash j_{j_2} \perp j_{j_2} : \gamma_2$</td>
</tr>
</tbody>
</table>

$$
\text{extract-assns}(\cdot) = \cdot
$$
$$
\text{extract-assns}(\Gamma, P) = \text{extract-assns}(\Gamma), P
$$
$$
\text{extract-assns}(\Gamma, \text{tt}) = \text{extract-assns}(\Gamma)
$$
$$
\text{extract-assns}(\Gamma, (P_1 \text{ and } \cdots \text{ and } P_n)) = \text{extract-assns}(\Gamma), P_1, \ldots, P_n
$$

for $n \geq 1$, where each $P_k$ has the form $\vdash a : \gamma$ or $a \equiv j : \gamma$

$$
\text{extract-assns}(\Gamma, Z) = \text{extract-assns}(\Gamma) \text{ where } Z \text{ is not a proposition}
$$
$$
\text{extract-ctx}(\cdot) = \cdot
$$
$$
\text{extract-ctx}(\Gamma, a : \gamma) = \text{extract-ctx}(\Gamma), (a \equiv a : \gamma)
$$
$$
\text{extract-ctx}(\Gamma, \alpha : \text{type}) = \text{extract-ctx}(\Gamma)
$$
$$
\text{extract-ctx}(\Gamma, d : K) = \text{extract-ctx}(\Gamma)
$$
$$
\text{extract-ctx}(\Gamma, p : \cdots) = \text{extract-ctx}(\Gamma)
$$
$$
\text{extract-ctx}(\Gamma, x : A) = \text{extract-ctx}(\Gamma)
$$
$$
\text{extract-ctx}(\Gamma, P) = \text{extract-ctx}(\Gamma)
$$
$$
\text{extract}(\Gamma) = (\text{extract-assns}(\Gamma) ; \text{extract-ctx}(\Gamma))
$$

Fig. 28. Extraction function on typing contexts

The next two definitions bridge the gap with the type system, in which contexts $\Gamma_T$ also include propositions $P$. It is defined assuming that $\text{extract}(\Gamma_T)$ (defined in Figure 28) has given us some propositions $P_1, \ldots, P_n$ and a relational context $\Gamma$.

**Definition F.6** (Extended semantic equivalence of index terms).
We define $P_1, \ldots, P_n; \Gamma \vdash i \equiv j : \gamma$ to hold if and only if $\mathcal{I}(P_1)$ and $\cdots$ and $\mathcal{I}(P_n)$ implies $\Gamma \vdash i \equiv j : \gamma$

where $\mathcal{I}(i \Theta j : \gamma) = (\Gamma \vdash i \Theta j : \gamma)$.

**Definition F.7** (Extended semantic apartness of index terms).
We define $P_1, \ldots, P_n; \Gamma \vdash i \perp j : \gamma$ to hold if and only if $\mathcal{I}(P_1)$ and $\cdots$ and $\mathcal{I}(P_n)$ implies $\Gamma \vdash i \perp j : \gamma$
where $\mathcal{F}(i \Theta j : \gamma) = (\Gamma \vdash i \Theta j : \gamma)$.

When a typing context is weakened, semantic equivalence and apartness under the extracted context continue to hold:

**Lemma F.1 (Weakening of Semantic Equivalence and Apartness).**

If $\text{extract}(\Gamma_T) \vdash i_1 \equiv i_2 : \gamma$ (respectively $i_1 \perp i_2 : \gamma$) then $\text{extract}(\Gamma_T, \Gamma_T') \vdash i_1 \equiv i_2 : \gamma$ (respectively $i_1 \perp i_2 : \gamma$).

**Proof.** By induction on $\Gamma_T'$.

We prove the $\equiv$ part; the $\perp$ part is similar.

- If $\Gamma_T' = \cdot$, we already have the result.
- If $\Gamma_T' = (\Gamma', P)$ then:
  
  By i.h., $\text{extract}(\Gamma_T, \Gamma') \vdash i_1 \equiv i_2 : \gamma$.
  
  That is, $\text{extract-assns}(\Gamma_T, \Gamma'); \text{extract-ctx}(\Gamma_T, \Gamma', P) \vdash i_1 \equiv i_2 : \gamma$.
  
  By its definition, $\text{extract-ctx}(\Gamma_T, \Gamma', P) = \text{extract-ctx}(\Gamma_T, \Gamma', P)$.
  
  Therefore, we have $\text{extract-assns}(\Gamma_T, \Gamma'); \text{extract-ctx}(\Gamma_T, \Gamma', P) \vdash i_1 \equiv i_2 : \gamma$.

Adding an assumption before the semicolon only supplements the antecedent in Def. F.6, so

$$\text{extract-assns}(\Gamma_T, \Gamma', P); \text{extract-ctx}(\Gamma_T, \Gamma', P) \vdash i_1 \equiv i_2 : \gamma$$

which was to be shown.

- If $\Gamma_T' = (\Gamma', a : \gamma)$ then by i.h.,
  
  $$\text{extract}(\Gamma_T, \Gamma') \vdash i_1 \equiv i_2 : \gamma$$

By definition of $\text{extract-ctx},$

$$\text{extract-ctx}(\Gamma_T, \Gamma', a : \gamma) = \text{extract-ctx}(\Gamma_T, \Gamma'), a \equiv a : \gamma$$

By the i.h. and Def. F.4,

$$(\text{extract-ctx}(\Gamma_T, \Gamma')), I \vdash i_1 : \gamma$$

We need to show that $(\text{extract-ctx}(\Gamma_T, \Gamma', a : \gamma)). I \vdash i_1 : \gamma$, which follows by weakening on sorting. The “.2” part is similar.

Since $a$ does not occur in $i_1$ and $i_2$, applying longer substitutions that include $a$ to $i_1$ and $i_2$ does not change them; thus, we get the same $j_1$ and $j_2$ as for $\Gamma_T, \Gamma'$.

- In the remaining cases of $Z$ for $\Gamma_T' = (\Gamma', Z)$, neither $\text{extract-assns}$ nor $\text{extract-ctx}$ change, and the i.h. immediately gives the result.

\[\square\]
F.3 Deductive equivalence and apartness for index terms

The index terms $i$ and $j$ are equivalent at sort $\gamma$

$$\frac{(i \equiv j : \gamma) \in \Gamma}{\Gamma \vdash i \equiv j : \gamma} \quad \text{Eq-Var}$$

$$\frac{(\Gamma).1 \vdash i : \gamma \quad (\Gamma).2 \vdash i : \gamma}{\Gamma \vdash i \equiv i : \gamma} \quad \text{E-Refl}$$

$$\frac{\Gamma \vdash i \equiv j : \gamma}{\Gamma, \lambda a. i \equiv j : \gamma} \quad \text{Eq-Lam}$$

$$\frac{\Gamma \vdash i \equiv j : \gamma_1 \quad \Gamma \vdash i \equiv j : \gamma_2}{\Gamma \vdash i \equiv j : \gamma_1 \ast \gamma_2} \quad \text{Eq-Pair}$$

$$\frac{\Gamma \vdash i \equiv j : \gamma_1 \quad \Gamma \vdash i \equiv j : \gamma_2}{\Gamma \vdash i_1 \equiv i : \gamma_1 \implies \gamma_2} \quad \text{E-App}$$

$$\frac{\Gamma \vdash i \equiv j : \gamma_1 \quad \Gamma \vdash i \equiv j : \gamma_2}{\Gamma \vdash (\lambda a. i_1)i \equiv j : \gamma} \quad \text{Eq-\beta}$$

$$\frac{\Gamma \vdash M \equiv N : \text{Nm}}{\Gamma \vdash \{M\} \equiv \{N\} : \text{NmSet}} \quad \text{Eq-Single}$$

$$\frac{\Gamma \vdash M \equiv N : \text{Nm}}{\Gamma \vdash \{M\} \equiv \{N\} : \text{NmSet}} \quad \text{Eq-Map}$$

$$\frac{\Gamma \vdash M \equiv N : \text{Nm} \quad \Gamma \vdash X \equiv Y : \text{NmSet}}{\Gamma \vdash M[X] \equiv N[Y] : \text{NmSet}} \quad \text{Eq-FlatMap}$$

$$\frac{\Gamma \vdash i \equiv j : \text{Nm} \quad \Gamma \vdash X \equiv Y : \text{NmSet}}{\Gamma \vdash i[X] \equiv j[Y] : \text{NmSet}} \quad \text{Eq-Star}$$

Fig. 29. Deductive rules for showing that two index terms are equivalent.
The index terms $i$ and $j$ are apart at sort $\gamma$

\[
\frac{\Gamma \vdash a \perp b : \gamma}{\Gamma \vdash a \perp b : \gamma} \quad \text{Var}
\]

\[
\frac{\Gamma \vdash i_1 \perp j_1 : \gamma_1}{\Gamma \vdash (i_1, i_2) \perp (j_1, j_2) : \gamma_1 * \gamma_2} \quad \text{D-Proj}_1
\]

\[
\frac{\Gamma \vdash i_2 \perp j_2 : \gamma_2}{\Gamma \vdash (i_1, i_2) \perp (j_1, j_2) : \gamma_1 * \gamma_2} \quad \text{D-Proj}_2
\]

\[
\frac{\Gamma \vdash \lambda a. i \perp \lambda b. j : \gamma_1 \equiv \gamma_2}{\Gamma \vdash i_2 \perp j_2 : \gamma_2} \quad \text{D-Lam}
\]

\[
\frac{\Gamma \vdash i_1 \equiv j_1}{\Gamma \vdash i_1 \equiv j_1} \quad \text{D-Star}
\]

\[
\frac{\Gamma \vdash i \equiv j : \text{Nm} \equiv \text{Nm}}{\Gamma \vdash i \equiv j : \text{Nm} \equiv \text{Nm}} \quad \text{D-FlatMap}_1
\]

\[
\frac{\Gamma \vdash i \equiv j : \text{Nm} \equiv \text{Nm}}{\Gamma \vdash i \equiv j : \text{Nm} \equiv \text{Nm}} \quad \text{D-FlatMap}_2
\]

\[
\frac{\Gamma \vdash X \perp Y : \text{NmSet}}{\Gamma \vdash X \perp Y : \text{NmSet}} \quad \text{D-Apart}
\]

\[
\frac{\Gamma \vdash X \perp Y : \text{NmSet}}{\Gamma \vdash X \perp Y : \text{NmSet}} \quad \text{D-Map}
\]

\[
\frac{\Gamma \vdash X \perp Y : \text{NmSet}}{\Gamma \vdash X \perp Y : \text{NmSet}} \quad \text{D-Star}
\]

Fig. 30. Deductive rules for showing that two index terms are apart
G NORMALIZATION FOR NAME TERMS

We write "M halts" when there exists V such that M \downarrow_M V.

We write σ : Γ when, for all α ∈ dom(Γ), we have \cdot \vdash σ(α) : Γ(α). It follows that σ(α) is closed.

Definition G.1 (Rγ(M)).

(1) Rγ(M) if and only if γ \neq (γ_1 \xrightarrow{\text{Nm}} γ_2) and M halts.
(2) R_{γ_1 \xrightarrow{\text{Nm}} γ_2}(M) if and only if (i) M halts and
(ii) for all closed M', if Rγ_1(M') then Rγ_2(M M').


Proof. By induction on the derivation of Γ, a : γ_a ⊩ M : γ.

Lemma G.3 (Closedness). If M is closed and M \downarrow_M V then V is closed.

Proof. By induction on the derivation of M \downarrow_M V.


(1) If γ = Nm then V = n.
(2) If γ = (γ_1 \xrightarrow{\text{Nm}} γ_2) then V = (λa. M_0) and a : γ_1 ⊩ M_0 : γ_2.

Proof. By inspection of the given derivation.


Proof. By induction on the length of σ, using Lemma G.2 (Substitution).

Lemma G.6 (Type Preservation). If ⊩ M : γ and M \downarrow_M V then ⊩ V : γ.

Lemma G.7 (Preservation). If Rγ(M) and M \downarrow_M V then Rγ(V).

Proof. By induction on γ.

If γ does not have the form (γ_1 \xrightarrow{\text{Nm}} γ_2), then the only requirement is to show there exists V' such that V \downarrow_M V'. Let V' = V. Then V \downarrow_M V' by teval-value.

Otherwise, γ = (γ_1 \xrightarrow{\text{Nm}} γ_2), and we also have to show that for all closed M_1 such that Rγ_1(M_1), it is the case that Rγ_2(M M_1).

By definition of R, there exists V_1 such that M_1 \downarrow_M V_1. By i.h., Rγ_1(V_1).

\[
\begin{align*}
M & \downarrow_M V & \text{Above} \\
V & = (λa. M_0) & \text{By Lemma G.4 (Canonical Forms)} \\
M_1 & \downarrow_M V_1 & \text{Above} \\
[V_1/a]M_0 & \downarrow_M V_2 & \text{By i.h.} \\
M & \downarrow_M V_2 & \text{By teval-app}
\end{align*}
\]

Lemma G.8 (Normalization).

If Γ ⊩ M : γ and σ : Γ and, for all α ∈ dom(Γ), we have R_{γ(α)}(σ(α)), then Rγ([σ]M).


- Case

\[
\begin{align*}
Γ & ⊩ n : \text{Nm} & \text{M-const}
\end{align*}
\]
\[ (\alpha : \gamma) \in \Gamma \]

\[ \Gamma \vdash \alpha : \gamma \]

We have \( \Gamma(\alpha) = \gamma \). It is given that \( R_{\Gamma(\alpha)}(\sigma(\alpha)) \). Since \( \sigma(\alpha) = [\sigma]a \), we have \( R_{\gamma}[\sigma]a \), which was to be shown.

\[ \Gamma, \alpha : \gamma_1 \vdash M_0 : \gamma_2 \]

\[ \Gamma \vdash (\lambda \alpha. M_0) : (\gamma_1 \rightarrow \gamma_2) \]

Suppose that, for some closed \( M' \), we have \( R_{\gamma_1}(M') \). By the definition of \( R \), that means there exists \( V' \) such that \( M' \vdash M' \]

We need to show \( R_{\gamma_2}([\sigma]((\lambda \alpha. M_0) M')) \).

Let \( \sigma_\alpha = (\sigma, V'/\alpha) \).

\[ R_{\gamma_1}(V') \]

By Lemma G.7 (Preservation)

\[ \Gamma, \alpha : \gamma_1 \vdash M_0 : \gamma_2 \]

Subderivation

\[ R_{\gamma_2}([\sigma_\alpha]M_0) \]

By i.h. with \( \sigma_\alpha \) as \( \sigma \)

\[ \lambda \alpha. [\sigma]M_0 \vdash_M \lambda \alpha. [\sigma]M_0 \]

By teval-value

\[ M' \vdash_M V' \]

Above

\[ [\sigma_\alpha]M_0 \vdash_M V \]

By definition of \( R \)

\[ [\sigma_\alpha]M_0 = [V'/\alpha][\sigma]M_0 \]

By def. of subst.

\[ [\lambda \alpha. [\sigma]M_0] M' \vdash_M V \]

By teval-app

\[ M' = [\sigma]M' \]

\[ M' \]

Closed

\[ [\lambda \alpha. [\sigma]M_0] [\sigma]M' \vdash_M V \]

By above equation

\[ [\lambda \alpha. [\sigma]M_0] [\sigma]M' = ([\sigma]\lambda \alpha. M_0) [\sigma]M' \]

By def. of subst.

\[ [\sigma]((\lambda \alpha. M_0) M') \vdash_M V \]

By above equations

\[ R_{\gamma_2}([\sigma]((\lambda \alpha. M_0) M')) \]

By definition of \( R \)

\[ \Gamma \vdash M_1 : (\gamma' \rightarrow \gamma) \quad \Gamma \vdash M_2 : \gamma' \]

\[ \Gamma \vdash (M_1, M_2) : \gamma \]

\[ R_{\gamma'}([\sigma]M_1) \]

By i.h.

\[ R_{\gamma'}([\sigma]M_2) \]

By i.h.

\[ R_{\gamma}([\sigma]M_1 \mid [\sigma]M_2) \]

By definition of \( R \)

\[ R_{\gamma}([\sigma](M_1 \mid M_2)) \]

By def. of subst.
Theorem G.9 (Normalization). If $\Gamma \vdash M : \gamma$ then there exists $V$ such that $M \Downarrow_M V$.

Proof. By Lemma G.8 (Normalization), $R_\gamma(M)$.

By definition of $R$, there exists $V$ such that $M \Downarrow_M V$.  \(\square\)