# Alias Types for Recursive Data Structures *
# (Extended Version)

David Walker and Greg Morrisett

Cornell University

**Abstract**

Linear type systems permit programmers to deallocate or explicitly recycle memory, but they are severly restricted by the fact that they admit no aliasing. This paper describes a pseudo-linear type system that allows a degree of aliasing and memory reuse as well as the ability to define complex recursive data structures. Our type system can encode conventional linear data structures such as linear lists and trees as well as more sophisticated data structures including cyclic and doubly-linked lists and trees. In the latter cases, our type system is expressive enough to represent pointer aliasing and yet safely permit destructive operations such as object deallocation. We demonstrate the flexibility of our type system by encoding two common compiler optimizations: destination-passing style and Deutsch-Schorr-Waite or "link-reversal" traversal algorithms.

## 1 Introduction

Type-safe programming languages, such as Haskell, Java, and ML, do not give programmers control over memory management. In particular, these languages do not allow programmers to separate allocation and initialization of memory objects, nor do they allow explicit re-use of memory objects. Rather, allocation and initialization of objects are presented to the programmer as an atomic operation, and re-use of memory is achieved "under the covers" through garbage collection. In other words, memory management is achieved by meta-linguistic mechanisms that are largely outside the control of the programmer.

In type-unsafe languages such as C or C++, programmers have control over memory management so they can tailor routines for application-specific constraints, where the time and/or space overheads of general-purpose memory management mechanisms do not suffice. However, such languages have a far more complicated and error-prone programming model. In particular, neither the static type systems, the compilers, nor the run-time systems of these languages prevent the accidental use of uninitialized objects, or the accidental re-use of memory at an incompatible type. Such errors are extremely costly to diagnose and correct.

Our ultimate goal is to provide support for programmer-controlled memory management, without sacrificing type-safety, and without incurring significant overhead. In addition, we hope to discover general typing mechanisms and principles that allow greater lattitude in the design of low-level languages intended for systems applications or as the target of certifying compilers [22, 23]. In this paper, we take a step further towards these goals by developing a type system that gives fine-grained control over memory management, for a rich class of recursively defined datatypes. We demonstrate the power of the type system by showing how we can safely encode two important classes of optimization, destination-passing style and link-reversal traversals of data structures.

### 1.1 Background

One well-known principle for proving type safety is based upon *type-invariance of memory locations*. Simply put, this property says that, when allocated, a memory object should (conceptually) be stamped with its type, and that the type of the object should not change during evaluation. When this property is maintained, it is straightforward to prove a subject-reduction or type-preservation property (see for example [36, 11]), which is in turn crucial to establishing type-soundness. There are many examples from language design where this principle has been violated and resulted in an unsoundness. For instance, the naive treatment of polymorphic references in an ML-like language, or the covariant treatment of arrays in a Java-like language, both violate this basic principle.

From the type-invariance principle, it becomes clear why most type-safe languages do not support user-level initialization or memory recycling: the type $\tau$ of the memory object cannot change, so (1) it must initially have type $\tau$ and (2) must continue to have type $\tau$ after an evaluation step. Atomic allocation and initialization ensures the first invariant, and the lack of explicit re-cycling ensures the second. Thus, it appears that some meta-linguistic mechanism is necessary to achieve memory management when the type-invariance principle is employed.

Linear type systems [35, 33] employ a different principle to achieve subject-reduction. In a linear setting, the crucial invariant is that memory objects must have exactly one reference — that is, no object can be aliased. Unlike the traditional approach, the type of a memory object can change over time and thus, explicit initialization and re-cycling can be performed in the language. Unfortunately, the inability to share objects through aliasing can have a steep cost: Many common and efficient data structures that use sharing or involve cycles cannot be implemented.

In recent previous work, we considered a generalization of linear types that supported a very limited degree of aliasing [29]. Like linear type systems, our alias types supported separation of allocation and initialization, and explicit re-use of memory, but unlike linear approaches, some objects could have more than one reference. To achieve subject reduction, we tracked aliasing in the type system by giving memory objects unique names, and maintained the invariant that the names were unique. We found that alias types unified a number of ad-hoc features in our Typed Assembly

*This material is based on work supported in part by the AFOSR grant F49620-97-1-0013 and the National Science Foundation under Grant No. EIA 97-03470. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not reflect the views of these agencies.

Language, including the treatment of initialization and control stacks. Furthermore, the alias type constructors were easy to add to our type checker for TALx86 [31].

Unfortunately, the named objects in our alias-type system were restricted to a "second-class" status; though named objects could be passed to and from functions, the type system prevented a programmer from placing these objects in a recursive datatype such as a list or tree. The problem is that our type system did not track aliasing beyond a certain compile-time "frontier", and in this respect, was similar to the k-limiting approaches used in alias analysis [12]. As a result, we could not embed linear datatypes into our language, and the opportunities for user-level memory management were greatly reduced.

In this paper, we extend alias types to cover recursive datatypes in full generality. Our type system is powerful enough to encode linear variants of lists and trees, as well as richer data structures with complex shapes and aliasing relationships, such as cyclic or doubly-linked lists and trees. The critical addition to the type system is a mechanism for combining recursive type operators with first-class store abstractions that represent repeated patterns of aliasing. In this respect, our work is inspired by the more complex approaches to alias and shape analysis that have recently appeared in the literature [7, 9, 26].

The generalization to recursive datatypes opens the door for users or certifying compilers to have far more control over the memory management of complex data structures. To demonstrate this fact, we show how two classes of space optimization can be encoded in a language based on recursive alias types. The first optimization, called *destination-passing style* [34, 16, 5] transforms algorithms that are "tail-recursive modulo allocation" into properly tail-recursive algorithms, thereby avoiding the space overheads of a control stack. The second optimization shows how we can safely encode Deutsch-Schorr-Waite algorithms [28] for traversing a tree using minimal additional space, based on link-reversal.

In the following section, we motivate the type structure of the language by introducing a series of type-theoretic abstraction mechanisms that enable suitable approximations of the store. We then show how these constructors may be used to encode a number of common data structures, without losing the ability to explicitly manage memory. Section 3 formalizes these ideas by presenting the syntax and static semantics of a programming language that includes instructions for allocating, deallocating, and overwriting memory objects. Section 4 shows how the destination-passing style and link-reversal optimizations can be safely encoded in the language. Section 5 presents an operational semantics for the language and states a type soundness theorem. We close in Section 6 by further discussing related work.

## 2 Types for describing store shapes

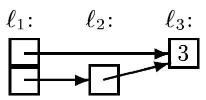
The linear type $\tau_1 \otimes \tau_2$ captures an extremely valuable memory management invariant: There is only one access path to any value with this type. Consequently, if $x$ has type $\tau_1 \otimes \tau_2$ then once both its components have been extracted, it is safe to reuse $x$ to store new values with incompatible types. Since the only way to access $x$'s data is through $x$ itself, there is no chance that this reuse can introduce inconsistent views of the store and unsoundness into the system.

Unfortunately, the restriction to a single access path makes it impossible to construct a number of important data structures. Our goal is to lift this restriction and yet retain the capacity to reuse or deallocate memory when there is a pointer to it. Our approach is based on the intuition that a linear data structure may be decomposed into two parts, a piece of state and a pointer to that state. Destructive operations such as memory reuse alter only the state component and leave the pointer part unchanged. Consequently, if the goal is to ensure no inconsistencies arise, only the state component need be treated linearly. The pointer may be freely copied, making it possible to construct complex data structures with shared parts. Of course, in order to actually *use* a pointer, there must be some way to relate it to the state it points to. We make this relationship explicit in the type system by introducing locations, $\ell$, that contain the state component, and by specializing the type of a pointer to indicate the location it points to. Consider again the linear pair $\tau_1 \otimes \tau_2$. We factor it into two parts:

- A type for the state, called an *aliasing constraint* or *store description*, that takes the form $\{\ell \mapsto \langle \tau_1, \tau_2 \rangle\}$. This type states that at location $\ell$ there exists a memory block containing objects with types $\tau_1$ and $\tau_2$.
- A type for a pointer to the location: $ptr(\ell)$. This type is a *singleton type*—any pointer described by this type is a pointer to the one location $\ell$ and to no other location.

This simple trick provides a tremendous flexibility advantage over conventional linear type systems because even though constraints may not alias one another, there is no explicit restriction on the way pointer types may be manipulated.

We build complicated data structures by joining a number of aliasing constraints together using the $\otimes$ constructor. For example, the following DAG may be specified by the constraints below.




$$\begin{array}{l}\{\ell_1 \mapsto \langle ptr(\ell_2), ptr(\ell_3)\rangle\} \otimes \\ \{\ell_2 \mapsto \langle ptr(\ell_3)\rangle\} \otimes \\ \{\ell_3 \mapsto \langle int \rangle\}\end{array}$$

In this type, the locations $\ell_1$, $\ell_2$ and $\ell_3$ are necessarily distinct from one another because they all appear on left-hand sides in this collection of constraints. The type system maintains the invariant that if a store is described by constraints $\{\ell_1 \mapsto \tau_1\} \otimes \cdots \otimes \{\ell_n \mapsto \tau_n\}$ then each of the locations $\ell_i$ must be different from one another. This invariant resembles invariants for the typing context of a standard linear type system. For example, the linear context $x_1{:}\tau_1, \ldots, x_n{:}\tau_n$ implies that the $x_i$ are distinct values with linear types $\tau_i$. However, the analogy is not exact because a linear type system prevents any of the $x_i$ from being used more than once whereas our calculus allows pointers to the locations $\ell_i$ to be used over and over again and this flexibility makes it possible to represent aliasing: In the type above, there are two paths from location $\ell_1$ to location $\ell_3$, one direct and one indirect through location $\ell_2$.

One other important invariant is that although the $\otimes$ constructor is reminiscent of linear pairs, the ordering of the constraints joined by $\otimes$ is not important: $\{\ell_1 \mapsto \tau_1\} \otimes \{\ell_2 \mapsto \tau_2\}$ is equivalent to $\{\ell_2 \mapsto \tau_2\} \otimes \{\ell_1 \mapsto \tau_1\}$. For the sake of brevity, we often abbreviate $\{\ell_1 \mapsto \tau_1\} \otimes \{\ell_n \mapsto \tau_n\}$ with $\{\ell_1 \mapsto \tau_1, \ldots, \ell_n \mapsto \tau_n\}$.

### 2.1 Abstraction mechanisms

Any particular store can be represented exactly using these techniques[1], even stores containing cyclic data structures. For example, a node containing a pointer to itself may be represented with the type $\{\ell \mapsto \langle ptr(\ell)\rangle\}$. However, the principle difficulty in describing aliasing relationships is not specifying one particular store but being able to specify a class of stores using a single compact representation. We use the following type-theoretic abstraction mechanisms to describe a wide class of pointer-rich data structures.

**Location Polymorphism** In general, the particular location $\ell$ that contains an object is inconsequential to the algorithm being executed. The relevant information is the connection between the location $\ell$, the contents of the memory residing there, and the pointers $ptr(\ell)$ to that location. Routines that only operate on specific concrete locations are almost useless. If, for example, the dereference function could only operate on a single concrete location $\ell$, we would have to implement a different dereference function for every location we allocate in the store! By introducing *location polymorphism*, it is possible to abstract away from the concrete location $\ell$ using a variable location $\rho$, but retain the necessary dependencies. We use the meta-variable $\eta$ to refer to locations generically (either concrete or variable).

**Store Polymorphism** Any specific routine only operates over a portion of the store. In order to use that routine in multiple contexts, we abstract irrelevant portions of the store using *store polymorphism*. A store described by the constraints $\epsilon \otimes \{\eta \mapsto \tau\}$ contains some store of unknown size and shape $\epsilon$ as well as a location $\eta$ containing objects with type $\tau$. We use the meta-variable $C$ to range over aliasing constraints in general.

**Unions** Unlike polymorphic types, unions provide users with the abstraction of one of a finite number of choices. A memory block that holds either an integer or a pointer may be encoded using the type $\langle int\rangle \cup \langle ptr(\eta)\rangle$. However, in order to use the contents of the block safely, there must be some way to detect which element of the union the underlying value actually belongs to. There are several ways to perform this test: through a pointer equality test with an object of known type, by descriminating between small integers (including null/0) and pointers, or by distinguishing between components using explicit tags. All of these options will be useful in an implementation, but here we concentrate on the third option. Hence, the alternatives above will be encoded using the type $\langle \mathcal{S}(1), int\rangle \cup \langle \mathcal{S}(2), ptr(\eta)\rangle$ where $\mathcal{S}(i)$ is another form of singleton type — the type containing only the integer $i$.

**Recursion** As yet, we have defined no mechanism for describing regular repeated structure in the store. We use standard recursive types of the form $\mu\alpha.\tau$ to capture this notion. However, recursion by itself is not enough. Consider an attempt to represent a store containing a linked list in the obvious way: $\{\eta \mapsto \mu\alpha.\langle \mathcal{S}(1)\rangle \cup \langle \mathcal{S}(2), \alpha\rangle\}$.[2] An unfolding of this definition results in the type $\{\eta \mapsto \langle \mathcal{S}(1)\rangle \cup \langle \mathcal{S}(2), \langle \mathcal{S}(1)\rangle \cup \langle \mathcal{S}(2), List\rangle\rangle\}$, rather than the type $\{\eta \mapsto \langle \mathcal{S}(1)\rangle \cup \langle \mathcal{S}(2), ptr(\eta')\rangle, \eta' \mapsto \langle \mathcal{S}(1)\rangle \cup \langle \mathcal{S}(2), List\rangle\}$. The former type describes a number of memory blocks flattened into the same location whereas the latter type describes a linked collection of disjoint nodes.

[1] We cannot represent a store containing a pointer into the middle of a memory block.

[2] Throughout we use the convention that union binds tighter than the recursion operator.

**Encapsulation** In order to represent linked recursive structures properly, each unfolding must encapsulate its own portion of the store. We use an existential type for this purpose. Hence, a sensible representation for linked lists is

$$\mu\alpha.\langle \mathcal{S}(1)\rangle \cup \exists[\rho{:}\texttt{Loc} \mid \{\rho \mapsto \alpha\}].\langle \mathcal{S}(2), ptr(\rho)\rangle$$

The existential $\exists[\rho{:}\texttt{Loc} \mid \{\rho \mapsto \tau_1\}].\tau_2$ may be read "there exists some location $\rho$, different from all others in the program, such that $\rho$ contains an object of type $\tau_1$, and the value contained in this data structure has type $\tau_2$. More generally, an existential has the form $\exists[\Delta \mid C].\tau$. It abstracts a sequence of type variables with their kinds, $\Delta$, and encapsulates a store described by some constraints $C$. In our examples, we will omit the kinds from the sequence $\Delta$ as they are clear from context. A similar definition gives rise to trees:

$$\mu\alpha.\langle \mathcal{S}(1)\rangle \cup \exists[\rho_1, \rho_2 \mid \{\rho_1 \mapsto \alpha, \rho_2 \mapsto \alpha\}].\\ \langle \mathcal{S}(2), ptr(\rho_1), ptr(\rho_2)\rangle$$

Notice that the existential abstracts a pair of locations and that both locations are bound in the store. From this definition, we can infer that the two subtrees are disjoint. For the sake of contrast, a DAG in which every node has a pair of pointers to a single successor is coded as follows. Here, reuse of the same location variable $\rho$ indicates aliasing.

$$\mu\alpha.\langle \mathcal{S}(1)\rangle \cup \exists[\rho \mid \{\rho \mapsto \alpha\}].\langle \mathcal{S}(2), ptr(\rho), ptr(\rho)\rangle$$

Cyclic lists and trees with leaves that point back to their roots also cause little problem—simply replace the terminal node with a memory block containing a pointer type back to the roots.

$$\begin{aligned} &CircularList = \\ &\quad \{\rho_1 \mapsto \mu\alpha.\langle \mathcal{S}(1), ptr(\rho_1)\rangle \cup \\ &\qquad\qquad \exists[\rho_2 \mid \{\rho_2 \mapsto \alpha\}].\langle \mathcal{S}(2), ptr(\rho_2)\rangle\} \end{aligned}$$

$$\begin{aligned} &CircularTree = \\ &\quad \{\rho_1 \mapsto \mu\alpha.\langle \mathcal{S}(1), ptr(\rho_1)\rangle \cup \\ &\qquad\qquad \exists[\rho_2, \rho_3 \mid \{\rho_2 \mapsto \alpha, \rho_3 \mapsto \alpha\}].\\ &\qquad\qquad\quad \langle \mathcal{S}(2), ptr(\rho_2), ptr(\rho_3)\rangle\} \end{aligned}$$

**Parameterized Recursive Types** One common data structure we are unable to encode with the types described so far is the doubly-linked list. Recursive types only "unfold" in one direction, making it easy to represent pointers from a parent "down" to its children, or all the way back up to the top-level store, but much more difficult to represent pointers that point back up from children to their parents, which is the case for doubly-linked lists or trees with pointers back to their parent nodes. Our solution to this problem is to use parameterized recursive types to pass a parent location down to its children. In general, a parameterized recursive type has the form $\texttt{rec}\,\alpha\,(\beta_1{:}\kappa_1, \ldots, \beta_n{:}\kappa_n).\tau$ and has kind $(\kappa_1, \ldots, \kappa_n) \to \texttt{Type}$. We will continue to use unparameterized recursive types $\mu\alpha.\tau$ in examples and consider them to be an abbreviation for $\texttt{rec}\,\alpha\,().\tau[\alpha\,()/\alpha]$. Once again, kinds will be omitted when they are clear from the context. Trees in which each node has a pointer to its parent may be encoded as follows.

$$\begin{array}{l}\{\rho_{root} \mapsto \langle \mathcal{S}(2), ptr(\rho_L), ptr(\rho_R)\rangle\} \otimes \\ \{\rho_L \mapsto REC\,(\rho_{root}, \rho_L)\} \otimes \\ \{\rho_R \mapsto REC\,(\rho_{root}, \rho_R)\}\end{array}$$

where

$$\begin{array}{l}REC = \\ \quad \mathtt{rec}\,\alpha\,(\rho_{prt}, \rho_{curr}). \\ \quad\quad \langle \mathcal{S}(1), ptr(\rho_{prt})\rangle \cup \\ \quad\quad \exists[\rho_L, \rho_R \mid \{\rho_L \mapsto \alpha\,(\rho_{curr}, \rho_L)\} \otimes \\ \quad\quad\quad\quad\quad \{\rho_R \mapsto \alpha\,(\rho_{curr}, \rho_R)\}]. \\ \quad\quad\quad\quad\quad\quad \langle \mathcal{S}(2), ptr(\rho_L), ptr(\rho_R), ptr(\rho_{prt})\rangle\end{array}$$

The tree has a root node in location $\rho_{root}$ that points to a pair of children in locations $\rho_L$ and $\rho_R$, each of which are defined by the recursive type $REC$. $REC$ has two arguments, one for the location of its immediate parent $\rho_{prt}$ and one for the location of the current node $\rho_{curr}$. Either the current node is a leaf, in which case it points back to its immediate parent, or it is an interior node, in which case it contains pointers to its two children $\rho_L$ and $\rho_R$ as well as a pointer to its parent. The children are defined recursively by providing the location of the current node ($\rho_{curr}$) for the parent parameter and the location of the respective child ($\rho_L$ or $\rho_R$) for the current pointer.

**Function Types** Functions are polymorphic with type arguments $\Delta$ and they express the shape of the store ($C$) required by the function: $\forall[\Delta \mid C].(\tau_1, \ldots, \tau_n)\rightarrow\mathbf{0}$. The underlying term language will be written in continuation-passing style and therefore functions never return, but instead call another function (the function's continuation). We use the notation "$\rightarrow\mathbf{0}$" to indicate this fact. Continuation-passing style is extremely convenient in this setting because it makes the flow of control explicit in the language and the store shape varies from one control-flow point to the next.

### 2.2 Summary of Type Structure

The formal syntax for the type constructor language is defined in the table below. We distinguish a subset of the types, called small types, for which no additional storage need be allocated when they are copied. The small types contain objects such as integers, functions[3] and data pointers. Function parameters are required to contain small types because function application is modeled by substitution, which copies values. Likewise, fields of memory blocks must be small because field projection copies values.

$$\begin{array}{llll}
\textit{kinds} & \kappa & ::= & \mathtt{Loc} \mid \mathtt{Store} \mid \mathtt{Small} \mid \mathtt{Type} \mid \\
& & & (\kappa_1, \ldots, \kappa_n) \rightarrow \mathtt{Type} \\
\textit{con. vars} & \beta & ::= & \rho \mid \epsilon \mid \alpha \\
\textit{con. ctxts} & \Delta & ::= & \cdot \mid \Delta, \beta{:}\kappa \\
\textit{constructors} & c & ::= & \eta \mid C \mid \tau \\
\textit{locations} & \eta & ::= & \rho \mid \ell \\
\textit{constraints} & C & ::= & \emptyset \mid C \otimes \{\eta \mapsto \tau\} \mid C \otimes \epsilon \\
\\
\textit{types} & \tau & ::= & \alpha \mid \sigma \mid \langle \sigma_1, \ldots, \sigma_n\rangle \mid \\
& & & \tau_1 \cup \tau_2 \mid \exists[\Delta \mid C].\tau \mid \\
& & & \mathtt{rec}\,\alpha\,(\Delta).\tau \mid c\,(c_1, \ldots, c_n) \\
\textit{small types} & \sigma & ::= & \alpha \mid int \mid \mathcal{S}(i) \mid ptr(\eta) \mid \\
& & & \forall[\Delta \mid C].(\sigma_1, \ldots, \sigma_n) \rightarrow \mathbf{0}
\end{array}$$

A judgement $\Delta \vdash c : \kappa$ states that a type is well-formed and has kind $\kappa$ according to the assignment of free type variables to kinds given by $\Delta$. Locations have kind `Loc`, aliasing constraints have kind `Store`, small types have the kind `Small`, but like the other types, may also be given kind `Type`. Recursive types have arrow kinds that can be eliminated through constructor application $c\,(c_1, \ldots, c_n)$. The judgement $\Delta \vdash c_1 = c_2 : \kappa$ states that type constructors $c_1$ and $c_2$ are equivalent and well-formed with kind $\kappa$. Types are considered equivalent up to alpha-conversion of bound variables and constraints are considered equivalent up to reordering of the elements in the sequence. A recursive type is not considered equal to its unfolding. The formal rules for these judgements are straightforward and they appear in Appendix A.

We use the notation $A[X/x]$ to denote the capture-avoiding substitution of $X$ for a variable $x$ in $A$. Occasionally, we use the notation $X[c_1, \ldots, c_n/\Delta]$ to denote capture-avoiding substitution of constructors $c_1, \ldots, c_n$ for the corresponding type variables in the domain of $\Delta$. Substitution is defined in the standard way in all cases except for the substitution of constraints in constraints. Substitution of $C'$ for a constraint variable $\epsilon$ in $C$ appends the list $C'$ to the list $C$. We use the notation $C'@C$ to denote the result of appending $C$ to $C'$ (notice that $C \otimes C'$ is not syntactically well-formed). For example,

$$\begin{array}{c}(\emptyset \otimes a_1 \otimes \cdots \otimes a_m)@(\emptyset \otimes a'_1 \otimes \cdots \otimes a'_n) = \\ \emptyset \otimes a_1 \otimes \cdots \otimes a_m \otimes a'_1 \otimes \cdots \otimes a'_n\end{array}$$

Formally, substitution for constraints is defined as follows.

$$(C \otimes \epsilon)[C'/\epsilon] = (C[C'/\epsilon])@C'$$

We will continue to omit the initial "$\emptyset$" when a constraint is non-empty. For example, we write $\{\eta \mapsto \tau\}$ instead of $\emptyset \otimes \{\eta \mapsto \tau\}$.

## 3 Term Structure

The term structure is split into three classes: values, instructions, and coercions. The grammar below describes the syntax of the language.

$$\begin{array}{llll}
\textit{values} & v & ::= & x \mid i \mid \mathcal{S}(i) \mid v[c] \mid \\
& & & \mathtt{fix}\,f[\Delta \mid C](x_1{:}\sigma_1, \ldots, x_n{:}\sigma_n).\iota \\
\textit{instruct's} & \iota & ::= & \mathtt{new}\,\rho, x, i; \iota \mid \mathtt{free}\,v; \iota \mid \\
& & & \mathtt{let}\,x = (v).i; \iota \mid (v_1).i := v_2; \iota \mid \\
& & & \mathtt{case}\,v\,(\mathtt{inl} \Rightarrow \iota_1 \mid \mathtt{inr} \Rightarrow \iota_2) \mid \\
& & & v(v_1, \ldots, v_n) \mid \mathtt{halt}\,v \mid \\
& & & \mathtt{coerce}(\gamma); \iota \\
\textit{coercions} & \gamma & ::= & \mathtt{union}_{\tau_1 \cup \tau_2}(\eta) \mid \\
& & & \mathtt{roll}_{\mathtt{rec}\,\alpha\,(\Delta).\tau\,(c_1, \ldots, c_n)}(\eta) \mid \\
& & & \mathtt{unroll}(\eta) \mid \\
& & & \mathtt{pack}_{[c_1, \ldots, c_n \mid C]\,\mathtt{as}\,\exists[\Delta \mid C].\tau}(\eta) \mid \\
& & & \mathtt{unpack}\,\eta\,\mathtt{with}\,\Delta
\end{array}$$

[3] For the purposes of this paper, we ignore the space required by closures. The language is powerful enough to encode closure conversion in the style of Morrisett *et al.* [22]. If desired, closure environments can be represented as memory blocks and functions can be required to be closed.

$\boxed{\Delta; \Gamma \vdash v : \tau}$

$$\frac{}{\Delta; \Gamma \vdash x : \Gamma(x)} \qquad \frac{}{\Delta; \Gamma \vdash i : \mathit{int}} \qquad \frac{}{\Delta; \Gamma \vdash \mathcal{S}(i) : \mathcal{S}(i)}$$

$$\frac{\Delta \vdash \forall[\Delta' \mid C'].(\sigma_1, \ldots, \sigma_n) \to \mathbf{0} = \sigma_f : \mathtt{Small} \quad \Delta\Delta'; C'; \Gamma, f{:}\sigma_f, x_1{:}\sigma_1, \ldots, x_n{:}\sigma_n \vdash \iota}{\Delta; \Gamma \vdash \mathtt{fix} f[\Delta' \mid C'](x_1{:}\sigma_1, \ldots, x_n{:}\sigma_n).\iota : \sigma_f}$$

$$\frac{\Delta; \Gamma \vdash v : \forall[\beta{:}\kappa, \Delta' \mid C'].(\sigma_1, \ldots, \sigma_n) \to \mathbf{0} \quad \Delta \vdash c : \kappa}{\Delta; \Gamma \vdash v[c] : (\forall[\Delta' \mid C'].(\sigma_1, \ldots, \sigma_n) \to \mathbf{0})[c/\beta]}$$

$$\frac{\Delta; \Gamma \vdash v : \sigma' \quad \Delta \vdash \sigma' = \sigma : \mathtt{Small}}{\Delta; \Gamma \vdash v : \sigma} \qquad \frac{\Delta; \Gamma \vdash v : \tau' \quad \Delta \vdash \tau' = \tau : \mathtt{Type}}{\Delta; \Gamma \vdash v : \tau}$$

Figure 1: Static Semantics: Values

**Values** Values consist of integers, singleton integers, and functions. Their typing judgements have the form $\Delta; \Gamma \vdash v : \tau$ where $\Gamma$ is a finite partial map from value variables to small types. The rules are mostly standard and are presented in figure 1. Notice that functions may be recursive and contain a specification of the polymorphic variables $\Delta$, the requirements on the store $C$ and the types of the parameters. These preconditions are used to type the instruction sequence that forms the body of the function. The value $v[c]$ denotes type application of the polymorphic function $v$ to type constructor $c$. We often abbreviate successive type applications $v[c_1] \cdots [c_n]$ by $v[c_1, \ldots, c_n]$. Later, when we give an operational semantics for the language, we will add other values (such as pointers and memory blocks), but these objects only appear at run time and so we omit them for now.

**Instructions** Figure 2 present the typing rules for the instructions. The judgement $\Delta; C; \Gamma \vdash \iota$ states that in type context $\Delta$, a store described by $C$ and value context $\Gamma$, the instruction sequence $\iota$ is well-formed.

The principle interest of the language is the typing of memory management instructions. Operationally, the $\mathtt{new}\ \rho, x, i$ instruction allocates a memory block of size $i$ at a fresh location and substitutes the location for $\rho$ and a pointer to that location for $x$ in the remaining instructions.[4] This operation is modeled in the type system by extending the store description with a memory type of length $i$. Initially, the fields of the memory block have type $\mathcal{S}(0)$ since we assume the allocator returns zeroed-out memory.[5] Once a block has been allocated, it may be operated on by accessor functions $\mathtt{let}\ x = (v_1).i$ and $(v_1).i := v_2$, which project from or store into the $i^{th}$ field of $v_1$. The projection operation is well-formed if $v_1$ is a pointer to some location $\eta$ and that location contains a object with type $\langle \sigma_1, \ldots, \sigma_n \rangle$ (where $i$ is less than $n$). In this case, the remaining instructions $\iota$ must be well-formed given the additional assumption that $x$ has type $\sigma_i$. The update operation is similar in that $v_1$ must be a pointer to a location containing a memory block. However, the remaining instructions are verified in a context where the type of the memory block has changed: The $i^{th}$ field has type $\sigma$ where $\sigma$ is the type of the object being stored into that location, but is otherwise unconstrained. Although surprising at first, this rule is sound because the constraints behave linearly. Despite the fact that the type of a memory block at a location changes, each location can only appear once in the domain of a store type and therefore there is no opportunity to introduce inconsistencies into the store typing. Constraints such as $\{\eta \mapsto \tau\} \otimes \{\eta \mapsto \tau'\}$ will never describe a well-formed store. The instruction $\mathtt{free}\ v$ frees the memory block pointed to by $v$. This effect is reflected in the typing rule for free by requiring that the remaining instructions be well-formed in a context $C'$ that does not include the location $\eta$.

The typing of the case expression is also somewhat unusual. Operationally, case checks the first field of the memory block in the location pointed to by a value $v$. If the first field is a 1, execution continues with the first instruction sequence, and if it is a 2, execution continues with the second instruction sequence. However the memory type constructor $\langle \cdots \rangle$ will not be the top-most type constructor (otherwise, the case would be unnecessary). The type system expects a union type to be the top-most and each alternative may contain some number (possibly zero) of existential quantifiers to abstract the store encapsulated in that alternative. The underlying memory value must have either tag 1 or tag 2 in its first field. As mentioned earlier, it is possible to formulate other union elimination constructs including pointer equality checks or discrimination between pointers and small integers (such as null implemented by 0).

Because the language has been defined in continuation-passing style, all instruction sequences are either terminated by a function call $v(v_1, \ldots, v_n)$ or a call to the terminal continuation $\mathtt{halt}$, which requires an integer argument. Function calls are well-formed if the polymorphic function $v$ has been fully instantiated, the constraints in the current context equal the constraints required by the function, and the argument types match the types of the function parameters.

The last instruction $\mathtt{coerce}(\gamma)$ applies a typing coercion to the store. Coercions, unlike the other instructions are for type-checking purposes only. Intuitively, coercions may be erased before executing a program and the run-

[4]For the purposes of alpha-conversion, $\rho$ and $x$ are considered bound by this instruction.

[5]If an allocator returns unzeroed, random memory, it is may be modelled by adding a Top type and returning a memory block with fields of type Top.

$\boxed{\Delta; C; \Gamma \vdash \iota}$

$$\frac{\Delta, \rho{:}\mathtt{Loc}; C \otimes \{\rho \mapsto \langle \overbrace{\mathcal{S}(0), \ldots, \mathcal{S}(0)}^{i} \rangle\}; \Gamma, x{:}ptr(\rho) \vdash \iota}{\Delta; C; \Gamma \vdash \mathtt{new}\ \rho, x, i; \iota} \ (x \notin Dom(\Gamma), \rho \notin Dom(\Delta))$$

$$\frac{\Delta; \Gamma \vdash v : ptr(\eta) \quad \Delta \vdash C = C' \otimes \{\eta \mapsto \langle \sigma_1, \ldots, \sigma_n \rangle\} : \mathtt{Store} \quad \Delta; C'; \Gamma \vdash \iota}{\Delta; C; \Gamma \vdash \mathtt{free}\ v; \iota}$$

$$\frac{\Delta; \Gamma \vdash v : ptr(\eta) \qquad \Delta \vdash C = C' \otimes \{\eta \mapsto \langle \sigma_1, \ldots, \sigma_n \rangle\} : \mathtt{Store} \qquad \Delta; C; \Gamma, x{:}\sigma_i \vdash \iota}{\Delta; C; \Gamma \vdash \mathtt{let}\ x = (v).i; \iota} \ \begin{pmatrix} 1 \leq i \leq n \\ x \notin Dom(\Gamma) \end{pmatrix}$$

$$\frac{\begin{array}{cc} \Delta; \Gamma \vdash v_1 : ptr(\eta) & \Delta \vdash C = C' \otimes \{\eta \mapsto \langle \sigma_1, \ldots, \sigma_i, \ldots, \sigma_n \rangle\} : \mathtt{Store} \\ \Delta; \Gamma \vdash v_2 : \sigma & \Delta; C' \otimes \{\eta \mapsto \langle \sigma_1, \ldots, \sigma, \ldots, \sigma_n \rangle\}; \Gamma \vdash \iota \end{array}}{\Delta; C; \Gamma \vdash (v_1).i := v_2; \iota} \ (1 \leq i \leq n)$$

$$\frac{\begin{array}{c} \Delta; \Gamma \vdash v : ptr(\eta) \qquad \Delta \vdash C = C' \otimes \{\eta \mapsto \tau_1 \cup \tau_2\} : \mathtt{Store} \\ \Delta \vdash \tau_1 = \exists[\Delta'_1 \mid C'_1]. \cdots \exists[\Delta'_j \mid C'_j].\langle \mathcal{S}(1), \sigma'_1, \ldots, \sigma'_k \rangle : \mathtt{Type} \\ \Delta \vdash \tau_2 = \exists[\Delta''_1 \mid C''_1]. \cdots \exists[\Delta''_m \mid C''_m].\langle \mathcal{S}(2), \sigma''_1, \ldots, \sigma''_n \rangle : \mathtt{Type} \\ \Delta; C' \otimes \{\eta \mapsto \tau_1\}; \Gamma \vdash \iota_1 \qquad \Delta; C' \otimes \{\eta \mapsto \tau_2\}; \Gamma \vdash \iota_2 \end{array}}{\Delta; C; \Gamma \vdash \mathtt{case}\, v\, (\mathtt{inl}\ \Rightarrow \iota_1 \mid \mathtt{inr}\ \Rightarrow \iota_2)}$$

$$\frac{\Delta; \Gamma \vdash v : \forall[\cdot \mid C].(\sigma_1, \ldots, \sigma_n) \to \mathbf{0} \qquad \Delta; \Gamma \vdash v_1 : \sigma_1 \qquad \cdots \qquad \Delta; \Gamma \vdash v_n : \sigma_n}{\Delta; C; \Gamma \vdash v(v_1, \ldots, v_n)}$$

$$\frac{\Delta; \Gamma \vdash v : int}{\Delta; C; \Gamma \vdash \mathtt{halt}\, v}$$

$$\frac{\Delta; C \vdash \gamma \Longrightarrow \Delta'; C' \quad \Delta'; C'; \Gamma \vdash \iota}{\Delta; C; \Gamma \vdash \mathtt{coerce}(\gamma); \iota}$$

Figure 2: Static Semantics: Instructions

time behaviour will not be affected. The judgement form $\Delta; C \vdash \gamma \Longrightarrow \Delta'; C'$ indicates that a coercion is well-formed, extends the type context to $\Delta'$, and produces new store constraints $C'$. These judgements are presented in figure 3.

Each coercion operates on a particular store location $\eta$. The `union` coercion lifts the object at $\eta$ into a union type and the `roll`/`unroll` coercions witness the isomorphism between a recursive type and its unfolding. The coercion $\mathtt{pack}_{[c_1,\ldots,c_n \mid C'[c_1,\ldots,c_n/\Delta']]\mathtt{as}\ \exists[\Delta' \mid C'].\tau}(\eta)$ introduces an existential type by hiding the type constructors $c_1, \ldots, c_n$ and encapsulating the store described by $C'[c_1, \ldots, c_n/\Delta']$. The `unpack` coercion eliminates an existential type, augments the current constraints with the encapsulated $C'$, and extends the type context $\Delta$ with $\Delta'$, the hidden type constructors.

## 4 Applications

In this section, we show how our language can be used to encode two common programming patterns, the destination-passing style pattern, which constructs data structures efficiently and the Deutsch-Schorr-Waite or "link-reversal" patterns, which traverse data structures using minimal additional space.

### 4.1 Destination-Passing Style

An effective optimization for functional languages is the *destination-passing style* (DPS) transformation. Wadler [34] first realized that compilers could detect certain "almost-tail-recursive" functions and automatically transform such functions into more efficient tail-recursive functions. Since then several other researchers have studied various facets of this problem [16, 5, 18]. Our contribution is to provide a type system that can be used in a type-preserving compiler and is capable of verifying that the code resulting from the transformation is safe.

Append is the canonical example of a function suitable for DPS:

$$\boxed{\Delta; C \vdash \gamma \Longrightarrow \Delta'; C'}$$

$$\frac{\Delta \vdash C = C' \otimes \{\eta \mapsto \tau_i\} : \texttt{Store} \qquad \Delta \vdash \tau_1 : \texttt{Type} \qquad \Delta \vdash \tau_2 : \texttt{Type}}{\Delta; C \vdash \texttt{union}_{\tau_1 \cup \tau_2}(\eta) \Longrightarrow \Delta; C' \otimes \{\eta \mapsto \tau_1 \cup \tau_2\}} \ (\text{for } i = 1 \text{ or } 2)$$

$$\frac{\Delta \vdash \tau = (\texttt{rec}\,\alpha\,(\Delta').\tau')\,(c_1, \ldots, c_n) : \texttt{Type} \qquad \Delta \vdash C = C' \otimes \{\eta \mapsto \tau'[\texttt{rec}\,\alpha\,(\Delta').\tau'/\alpha][c_1, \ldots, c_n/\Delta']\} : \texttt{Store}}{\Delta; C \vdash \texttt{roll}_\tau(\eta) \Longrightarrow \Delta; C' \otimes \{\eta \mapsto \tau\}}$$

$$\frac{\Delta \vdash C = C' \otimes \{\eta \mapsto \tau\} : \texttt{Store} \qquad \Delta \vdash \tau = (\texttt{rec}\,\alpha\,(\Delta').\tau')\,(c_1, \ldots, c_n) : \texttt{Type}}{\Delta; C \vdash \texttt{unroll}(\eta) \Longrightarrow \Delta; C' \otimes \{\eta \mapsto \tau'[\texttt{rec}\,\alpha\,(\Delta').\tau'/\alpha][c_1, \ldots, c_n/\Delta']\}}$$

$$\frac{\begin{array}{c}\Delta' = \beta_1{:}\kappa_1, \ldots, \beta_n{:}\kappa_n \qquad \cdot \vdash c_i : \kappa_i \quad (\text{for } 1 \leq i \leq n) \\ \Delta \vdash C = C'' \otimes \{\eta \mapsto \tau[c_1, \ldots, c_n/\Delta']\} \otimes C'[c_1, \ldots, c_n/\Delta'] : \texttt{Store}\end{array}}{\Delta; C \vdash \texttt{pack}_{[c_1, \ldots, c_n \mid C'[c_1, \ldots, c_n/\Delta']]\,\texttt{as}\,\exists[\Delta' \mid C'].\tau}(\eta) \Longrightarrow \Delta; C'' \otimes \{\eta \mapsto \exists[\Delta' \mid C'].\tau\}}$$

$$\frac{\Delta \vdash C = C'' \otimes \{\eta \mapsto \exists[\Delta' \mid C'].\tau\} : \texttt{Store}}{\Delta; C \vdash \texttt{unpack}\,\eta\,\texttt{with}\,\Delta' \Longrightarrow \Delta, \Delta'; C'' \otimes \{\eta \mapsto \tau\} \mathbin{@} C'}$$

Figure 3: Static Semantics: Coercions

```
fun append (xs,ys) =
  case xs of
    [] -> []
  | hd :: tl -> hd :: append (tl,ys)
```

Here, the second-last operation in the second arm of the case is a function call and the last operation constructs a cons cell. If the two operations were inverted, we would have an efficient tail-recursive function. In DPS, the function allocates a cons cell before the recursive call and passes the partially uninitialized value to the function, which computes its result and fills in the uninitialized part of the data structure. If the input list `xs` is linear, it will not be used in the future. In this case, it is possible to further optimize the program by reusing the input list cells for the output list. Our example performs both of these optimizations.

Before presenting the code for the optimized function, we will need to define a number of abbreviations. Such abbreviations not only aid readability, but also help compress typing information in a compiler [10]. First, recall the type of integer lists $List$ and their unrolling $List'$:

$$\begin{array}{rcl} List & = & \mu\alpha.\langle\mathcal{S}(1)\rangle \cup \exists[\rho \mid \{\rho \mapsto \alpha\}].\langle\mathcal{S}(2), int, ptr(\rho)\rangle \\ List' & = & \langle\mathcal{S}(1)\rangle \cup \exists[\rho \mid \{\rho \mapsto List\}].\langle\mathcal{S}(2), int, ptr(\rho)\rangle \end{array}$$

Given these list definitions, it will be useful to define the following composite coercion.

$$\begin{array}{l}\texttt{rollList}\,\rho_1\,\texttt{packing}\,\rho_2 = \\ \quad \texttt{pack}_{[\rho_2 \mid \{\rho_2 \mapsto List\}]\,\texttt{as}\,\exists[\rho_2 \mid \{\rho_2 \mapsto List\}].\langle\mathcal{S}(2), int, ptr(\rho_2)\rangle}(\rho_1); \\ \quad \texttt{union}_{List'}(\rho_1); \\ \quad \texttt{roll}_{List}(\rho_1)\end{array}$$

This coercion operates on a portion of the store with shape $\{\rho_1 \mapsto \langle\mathcal{S}(2), int, ptr(\rho_2)\rangle\} \otimes \{\rho_2 \mapsto List\}$. It packs up $\rho_2$ into an existential around $\rho_1$, lifts the resultant object up to a union type and finally rolls it up, producing a store with the shape $\{\rho_1 \mapsto List\}$.

The function $append'$, presented in figure 4, implements the inner loop of the optimized append function. A wrapper function must check for the case that the input list is empty. If not, it passes two pointers to the beginning of the first list (aliases of one another) to $append'$ for parameters $prev$ and $start$. It also passes a pointer to the second element in that list for parameter $xs$ and a pointer to the second list for parameter $ys$. Notice that the contents of location $\rho_s$ are not described by the aliasing constraints. On the first iteration of the loop $\rho_s$ is an alias of $\rho_p$ and on successive iterations, it abstracted by $\epsilon$. However, these facts are not explicit in the type structure and therefore $\rho_s$ cannot be used during any iteration of the loop ($cont$ will be aware that $\rho_s$ equals $\rho_p$ and may use the resultant list).

The first place to look to understand this code is at the aliasing constraints, which act as a loop invariant. Reading the constraints in the type from left to right reveals that the function expects a store with some unknown part ($\epsilon$) as well as a known part. The known part contains a cons cell at location $\rho_p$ that is linked to a $List$ in location $\rho_{xs}$. Independent of either of these objects is a third location, $\rho_{ys}$, which also contains a $List$.

The first instruction in the function unrolls the recursive type of the object at $\rho_{xs}$ to reveal that it is a union and can be eliminated by a case statement. In the first branch of the case, $xs$ must point to null. The code frees the null cell, resulting in a store at program point `1` that can be described by the constraints $\epsilon \otimes \{\rho_p \mapsto \langle\mathcal{S}(2), int, ptr(\rho_{xs})\rangle\} \otimes \{\rho_{ys} \mapsto List\}$. Observe that the cons cell at $\rho_p$ contains a dangling pointer to memory location $\rho_{xs}$, the location that has just been freed and no longer appears in the constraints. Despite the dangling pointer, the code is perfectly safe: The typing rules prevent the pointer from being used.

Next, the second list $ys$ is banged into the cons cell at $\rho_p$.

$$
\begin{array}{l}
\texttt{fix}\, \mathit{append}'\, [\epsilon, \rho_{xs}, \rho_{ys}, \rho_p, \rho_s \mid \\
\quad \epsilon \otimes \{\rho_p \mapsto \langle \mathcal{S}(2), \mathit{int}, \mathit{ptr}(\rho_{xs})\rangle, \rho_{xs} \mapsto \mathit{List}, \rho_{ys} \mapsto \mathit{List}\}]. \\
\quad (xs : \rho_{xs}, ys : \rho_{ys}, \mathit{prev} : \mathit{ptr}(\rho_p), \mathit{start} : \mathit{ptr}(\rho_s), \\
\qquad \mathit{cont} : \tau_c[\epsilon, \rho_p, \rho_s])\,. \\
\quad \texttt{unroll}(\rho_{xs}); \\
\quad \texttt{case}\, xs \\
\qquad (\ \texttt{inl} \Longrightarrow \\
\qquad\qquad \texttt{free}\, xs; \qquad\qquad\qquad\qquad \texttt{\% 1.} \\
\qquad\qquad (\mathit{prev}).3 := ys; \qquad\qquad\quad\ \texttt{\% 2.} \\
\qquad\qquad \texttt{rollList}\, \rho_p\, \texttt{packing}\, \rho_{ys}; \quad \texttt{\% 3.} \\
\qquad\qquad \mathit{cont}(\mathit{start}) \\
\qquad \mid \texttt{inr} \Longrightarrow \\
\qquad\qquad \texttt{unpack}\, \rho_{xs}\, \texttt{with}\, \rho_{tl}\, ; \qquad\quad\ \texttt{\% 4.} \\
\qquad\qquad \texttt{let}\, tl = (xs).3; \qquad\qquad\quad \texttt{\% 5.} \\
\qquad\qquad \mathit{append}' \\
\qquad\qquad\quad [\epsilon \otimes \{\rho_p \mapsto \langle \mathcal{S}(2), \mathit{int}, \mathit{ptr}(\rho_{xs})\rangle\}, \rho_{tl}, \rho_{ys}, \rho_{xs}, \rho_s] \\
\qquad\qquad\quad (tl, ys, xs, \mathit{start}, \mathit{cont}')) \\
\\
\texttt{where}\ \ \tau_c[\epsilon, \rho_p, \rho_s] = \forall[\cdot \mid \epsilon \otimes \{\rho_p \mapsto \mathit{List}\}].(\mathit{ptr}(\rho_s)) \to \mathbf{0}
\end{array}
$$

Figure 4: Optimized Append

Hence, at program point 2, the store has a shape described by $\epsilon\otimes\{\rho_p \mapsto \langle\mathcal{S}(2), \mathit{int}, \mathit{ptr}(\rho_{ys})\rangle\}\otimes\{\rho_{ys} \mapsto \mathit{List}\}$. The type of the cons cell at $\rho_p$ is different here than at 1, reflecting the new link structure of store. The tail of the cell no longer points to location $\rho_{xs}$, but to $\rho_{ys}$ instead. After packing and rolling using the composite coercion, the store can be described by $\epsilon \otimes \{\rho_p \mapsto \mathit{List}\}$. This shape equals the shape expected by the continuation (see the definition of $\tau_c$), so the function call is valid.

In the second branch of the case, $xs$ must point to a cons cell. The existential containing the tail of the list is unpacked and at program point 4, the store has shape $\epsilon\otimes\{\rho_p \mapsto \langle\mathcal{S}(2), \mathit{int}, \mathit{ptr}(\rho_{xs})\rangle\}\otimes\{\rho_{xs} \mapsto \langle\mathcal{S}(2), \mathit{int}, \mathit{ptr}(\rho_{tl})\rangle\}\otimes\{\rho_{tl} \mapsto \mathit{List}\} \otimes \{\rho_{ys} \mapsto \mathit{List}\}$. It is now possible to project the tail of $xs$. To complete the loop, the code uses polymorphic recursion. At the end of the second branch, the constraint variable $\epsilon$ for the next iteration of the loop is instantiated with the current $\epsilon$ and the contents of location $\rho_p$, hiding the previous node in the list. The location variables $\rho_{xs}$ and $\rho_p$ are instantiated to reflect the shift to the next node in the list. The locations $\rho_{ys}$ and $\rho_s$ are invariant around the loop and therefore are instantiated with themselves.

The last problem is how to define the continuation $\mathit{cont}'$ for the next iteration. The function should be tail-recursive, so we would like to use the continuation $\mathit{cont}$. However, close inspection reveals that the next iteration of append requires a continuation with type $\tau_c[\epsilon \otimes \{\rho_p \mapsto \langle\mathcal{S}(2), \mathit{int}, \mathit{ptr}(\rho_{xs})\rangle\}, \rho_{xs}, \rho_s]$ but that the continuation $\mathit{cont}$ has type $\tau_c[\epsilon, \rho_p, \rho_s]$. The problem is that this iteration of the recursion has unrolled and unpacked the recursive data structure pointed to by $xs$, but before "returning" by calling the continuation, the list must be packed and rolled back up again. Therefore, the appropriate definition of $\mathit{cont}'$ is $\mathit{cont} \circ (\texttt{rollList}\, \rho_p\, \texttt{packing}\, \rho_{xs})$. Once the continuation packs $\rho_{xs}$ and rolls the contents of location $\rho_p$ into a $\mathit{List}$, the constraints satisfy the requirements of the continuation $\mathit{cont}$. Semantically, $\mathit{cont}'$ is equivalent to the following function.

$$
\begin{array}{l}
\texttt{fix}\, \_[\cdot \mid \epsilon \otimes \{\rho_p \mapsto \langle\mathcal{S}(2), \mathit{int}, \mathit{ptr}(\rho_{xs})\rangle\}\{\rho_{xs} \mapsto \mathit{List}\}] \\
\quad (\mathit{start}{:}\mathit{ptr}(\rho_s)). \\
\quad \texttt{rollList}\, \rho_p\, \texttt{packing}\, \rho_{xs}; \\
\quad \mathit{cont}(\mathit{start})
\end{array}
$$

However, because coercions can be erased before running a program, it is simple to arrange for $\mathit{cont}'$ to be implemented by $\mathit{cont}$.

### 4.2 Deutsch-Schorr-Waite Algorithms

Deutsch-Schorr-Waite or "link reversal" algorithms, are well-known algorithms for traversing data structures while incurring minimal additional space overhead. These algorithms were first developed for executing the mark phase of a garbage collector [28]. During garbage collection, there is little or no extra space available for storing control information, so minimizing the overhead of the traversal is a must. Recent work by Sobel and Friedman [30] has shown how to automatically transform certain continuation-passing style programs, those generated by *anamorphisms* [17], into link-reversal algorithms. Here we give an example how to encode a link-reversal algorithm in our calculus.

For this application, we will use the definition of trees from section 2.

$$
\begin{array}{l}
\mathit{Tree} = \\
\quad \mu\alpha.\langle\mathcal{S}(1)\rangle \cup \exists[\rho_L, \rho_R \mid \{\rho_L \mapsto \alpha, \rho_R \mapsto \alpha\}]. \\
\qquad\qquad \langle\mathcal{S}(2), \mathit{ptr}(\rho_L), \mathit{ptr}(\rho_R)\rangle
\end{array}
$$

$$
\begin{array}{l}
\mathit{Tree}' = \\
\quad \langle\mathcal{S}(1)\rangle \cup \exists[\rho_L, \rho_R \mid \{\rho_L \mapsto \mathit{Tree}, \rho_R \mapsto \mathit{Tree}\}]. \\
\qquad\qquad \langle\mathcal{S}(2), \mathit{ptr}(\rho_L), \mathit{ptr}(\rho_R)\rangle
\end{array}
$$

The code for the algorithm appears in figure 5. The trick to the algorithm is that when recursing into the left subtree, it uses space normally reserved for a pointer to that subtree to point back to the parent node. Similarly, when recursing into the right subtree, it uses the space for the right pointer. In both cases, it uses the tag field of the data structure to store a continuation that knows what to do next (recurse into right subtree or follow the parent pointers back up the tree). Before ascending back up out of the tree, the algorithm restores the link structure to a proper tree shape and the type system checks this is done properly. Notice that all of the functions and continuations are closed, so there is no stack hiding in the closures.

## 5 Operational Semantics and Type Soundness

In this section, we define the syntax and static semantics of the values manipulated at run-time, including pointers, memory blocks and the store and give an operational semantics for the language. The type system is sound with respect to this semantics.

**Run-time Values** The run-time values consist of all the values defined in previous sections as well as pointers $\texttt{ptr}(\ell)$, memory blocks $\langle v_1, \ldots, v_n\rangle$ and witnessed values $\varsigma(v)$. Witnessed values are introduced by coercions. For example, the union coercion introduces a union witness and similarly for roll and pack coercions. Notice that these values are always type checked in an empty type context and empty value context (evaluation of open terms is nonsensical).

```
% Traverse a tree node
letrec walk[ε, ρ1, ρ2 | ε ⊗ {ρ1 ↦ Tree}]
        (t : ptr(ρ1), up : ptr(ρ2), cont : τc[ε, ρ1, ρ2]).
  unroll(ρ1);
  case t of
    ( inl ⟹
        union_Tree'(ρ1);
        roll_Tree(ρ1);
        cont(t, up)
    | inr ⟹
        unpack ρ1 with ρL, ρR ;
        % store cont in tag position
        (t).1 := cont;
        let left = (t).2;
        % store parent pointer as left subtree
        (t).2 := up;
        walk[ε⊗
             {ρ1 ↦ ⟨τc[ε, ρ1, ρ2], ptr(ρ2), ptr(ρR)⟩}⊗
             {ρR ↦ Tree}, ρL, ρ1]
           (left, t, rwalk[ε, ρ1, ρ2, ρL, ρR]))

% Walk the right-hand subtree
and rwalk[ε, ρ1, ρ2, ρL, ρR | ε⊗
        {ρ1 ↦ ⟨τc[ε, ρ1, ρ2], ptr(ρ2), ptr(ρR)⟩}⊗
        {ρL ↦ Tree}⊗
        {ρR ↦ Tree}]
        (left : ptr(ρL), t : ptr(ρ1)).
  let up = (t).2;
  % restore left subtree
  (t).2 := left;
  let right = (t).3;
  % store parent pointer as right subtree
  (t).3 := up;
  walk[ε⊗
       {ρ1 ↦ ⟨τc[ε, ρ1, ρ2], ptr(ρL), ptr(ρ2)⟩}⊗
       {ρL ↦ Tree}, ρR, ρ1]
     (right, t, finish[ε, ρ1, ρ2, ρL, ρR])

% Reconstruct tree node and return
and finish[ε, ρ1, ρ2, ρL, ρR | ε⊗
         {ρ1 ↦ ⟨τc[ε, ρ1, ρ2], ptr(ρL), ptr(ρ2)⟩}⊗
         {ρL ↦ Tree}⊗
         {ρR ↦ Tree}]
         (right : ptr(ρR), t : ptr(ρ1)).
  let up = (t).3;
  % restore right subtree
  (t).3 := right;
  let cont = (t).1;
  % restore tag
  (t).1 := S(2);
  pack_{ρL,ρR}(ρ1);
  union_Tree'(ρ1);
  roll_Tree(ρ1);
  cont(t, up)

where τc[ε, ρ1, ρ2] =
    ∀[· | ε ⊗ {ρ1 ↦ Tree}].(ptr(ρ1), ptr(ρ2)) → 0
```

Figure 5: Deutsch-Schorr-Waite tree traversal with constant space overhead

$$
\begin{array}{llll}
\textit{values} & v & ::= & \cdots \mid \mathbf{ptr}(\ell) \mid \langle v_1, \ldots, v_n \rangle \mid \varsigma(v) \\
\textit{witnesses} & \varsigma & ::= & \mathtt{union}_{\tau_1 \cup \tau_2} \mid \\
 & & & \mathtt{pack}_{[c_1, \ldots, c_n \mid S] \mathtt{as} \exists [\Delta \mid C].\tau} \mid \\
 & & & \mathtt{roll}_{(\mathtt{rec}\, \alpha\, (\Delta).\tau)\, (c_1, \ldots, c_n)}
\end{array}
$$

$$
\frac{\cdot \vdash \tau_1 \cup \tau_2 : \mathtt{Type} \qquad \cdot; \cdot \vdash v : \tau_1 \quad \text{or} \quad \cdot; \cdot \vdash v : \tau_2}{\cdot; \cdot \vdash \mathtt{union}_{\tau_1 \cup \tau_2}(v) : \tau_1 \cup \tau_2}
$$

$$
\frac{\begin{array}{c} \cdot \vdash \tau = (\mathtt{rec}\, \alpha\, (\Delta).\tau')\, (c_1, \ldots, c_n) : \mathtt{Type} \\ \cdot; \cdot \vdash v : \tau'[\mathtt{rec}\, \alpha\, (\Delta).\tau'/\alpha][c_1, \ldots, c_n/\Delta] \end{array}}{\cdot; \cdot \vdash \mathtt{roll}_\tau(v) : \tau}
$$

$$
\frac{\begin{array}{ll} \Delta = \beta_1{:}\kappa_1, \ldots, \beta_n{:}\kappa_n & \cdot \vdash c_i : \kappa_i \quad (\text{for } 1 \leq i \leq n) \\ \vdash S : C[c_1, \ldots, c_n/\Delta] & \cdot; \cdot \vdash v : \tau[c_1, \ldots, c_n/\Delta] \end{array}}{\cdot; \cdot \vdash \mathtt{pack}_{[c_1, \ldots, c_n \mid S] \mathtt{as} \exists [\Delta \mid C].\tau}(v) : \exists [\Delta \mid C].\tau}
$$

The pack coercion encapsulates a portion of the store, $S$, which is a finite partial mapping from concrete locations to values. We treat stores equivalent up to reordering of their elements and use the notation $S\{\ell \mapsto v\}$ to denote the extension of $S$ to include the mapping $\{\ell \mapsto v\}$. The notation is undefined if $\ell \in \mathit{Dom}(S)$. The store well-formedness judgement is written $\vdash S : C$ and is given below.

$$
\frac{\begin{array}{c} S = \{\ell_1 \mapsto v_1, \ldots, \ell_n \mapsto v_n\} \\ \cdot \vdash C = \{\ell_1 \mapsto \tau_1, \ldots, \ell_n \mapsto \tau_n\} : \mathtt{Store} \\ \cdot; \cdot \vdash v_i : \tau_i \qquad (\text{for } 1 \leq i \leq n) \end{array}}{\vdash S : C}
$$

There are no duplicate locations in the domain of a store (otherwise, it would not be a finite partial map). However, we will require a stronger property of stores to prove that program evaluation cannot get stuck. Informally, there can be no duplication of locations in the domain of the store or in any encapsulated store. We call this property *Global Uniqueness.*

**Definition 1 (Global Uniqueness)** $\mathtt{GU}(S)$ *if and only if there are no duplicate locations in* $\mathtt{L}(S)$.

**Definition 2 (Global Store Locations)** $\mathtt{L}(S)$ *is the multi-set given by the following definition.*

$$
\begin{array}{l}
\mathtt{L}(\{\ell_1 \mapsto v_1, \ldots, \ell_n \mapsto v_n\}) \\
\quad = \{\ell_1, \ldots, \ell_n\} \uplus \mathtt{L}(v_1) \uplus \cdots \uplus \mathtt{L}(v_n) \\
\mathtt{L}(\mathtt{pack}_{[c_1, \ldots, c_n \mid S] \mathtt{as} \tau}(v)) \\
\quad = \mathtt{L}(S) \uplus \mathtt{L}(v)
\end{array}
$$

$$
\begin{array}{l}
\mathtt{L}(x) = \mathtt{L}(x_1) \uplus \cdots \uplus \mathtt{L}(x_n) \\
\quad \textit{for any other term construct } x \\
\quad \textit{where } x_1, \ldots, x_n \textit{ are the subcomponents of } x.
\end{array}
$$

A program is a store paired with an instruction stream. A program is well-formed, written $\vdash (S, \iota)$, under the following circumstances.

**Definition 3 (Well-formed Program)** $\vdash (S, \iota)$ *iff*

1. *The store adheres to global uniqueness* $\mathtt{GU}(S)$.
2. *There exists constraints* $C$ *such that* $\vdash S : C$.
3. *The instructions are well-formed with the given constraints:* $\cdot; C; \cdot \vdash \iota$.

$\boxed{(S,\iota) \longmapsto_P (S,\iota)}$

$$
\begin{array}{lcl}
(S, \texttt{new}\ \rho, x, i; \iota) & \longmapsto_P & (S\{\ell \mapsto v\}, \iota[\ell/\rho][\texttt{ptr}(\ell)/x]) \\
\quad \text{where } \ell \notin S, \iota \text{ and } v = \overbrace{\langle \mathcal{S}(0), \ldots, \mathcal{S}(0) \rangle}^{i} & & \\
(S\{\ell \mapsto \langle v_1, \ldots, v_n \rangle\}, \texttt{free ptr}(\ell); \iota) & \longmapsto_P & (S, \iota) \\
(S\{\ell \mapsto \langle v_1, \ldots, v_n \rangle\}, \texttt{let}\ x = (\texttt{ptr}(\ell)).i; \iota) & \longmapsto_P & (S\{\ell \mapsto \langle v_1, \ldots, v_n \rangle\}, \iota[v_i/x]) \\
\quad \text{where } 1 \le i \le n & & \\
(S\{\ell \mapsto \langle v_1, \ldots, v_i, \ldots, v_n \rangle\}, (\texttt{ptr}(\ell)).i := v'; \iota) & \longmapsto_P & (S\{\ell \mapsto \langle v_1, \ldots, v', \ldots, v_n \rangle\}, \iota) \\
\quad \text{where } 1 \le i \le n & & \\
(S\{\ell \mapsto v\}, \texttt{case ptr}(\ell)\,(\texttt{inl} \Rightarrow \iota_1 \mid \texttt{inr} \Rightarrow \iota_2)) & \longmapsto_P & (S\{\ell \mapsto v'\}, \iota_i) \\
\quad \begin{array}{lrcl} & i & = & 1 \text{ or } 2 \\ \text{where} & v & = & \texttt{union}_{\tau_1 \cup \tau_2}(\varsigma_1(\cdots \varsigma_m(\langle \mathcal{S}(i), v_1, \ldots, v_n \rangle) \cdots)) \\ & v' & = & \varsigma_1(\cdots \varsigma_m(\langle \mathcal{S}(i), v_1, \ldots, v_n \rangle) \cdots) \end{array} & & \\
(S, v(v_1, \ldots, v_n)) & \longmapsto_P & (S, \theta(\iota)) \\
\quad \begin{array}{lrcl} & v & = & v'[c_1, \ldots, c_m] \\ \text{where} & v' & = & \texttt{fix}\,f[\Delta \mid C](x_1{:}\sigma_1, \ldots, x_n{:}\sigma_n).\iota \\ & \theta & = & [c_1, \ldots, c_m/\Delta][v'/f][v_1, \ldots, v_n/x_1, \ldots, x_n] \end{array} & & \\
(S, \texttt{coerce}(\gamma); \iota) & \longmapsto_P & (S', \theta(\iota)) \\
\quad \text{where } \gamma(S) \longmapsto_\gamma S', \theta & &
\end{array}
$$

Figure 6: Operational Semantics: Programs

**Operational Semantics** The small-step operational semantics for the language is given by a function $P \longmapsto_P P'$. The majority of the operational rules are entirely standard and formalize the intuitive rules described earlier in the paper. The operational rule for the coerce instruction depends upon a separate semantics for coercions that has the form $S \longmapsto_\gamma S', \theta$ where $\theta$ is a substitution of type constructors for type constructors variables. Inspection of these rules reveals that coercions do not alter the association between locations and memory blocks; they simply insert witnesses that alter the typing derivation so that it is possible to prove a type soundness result. The rules for program and coercion operational semantics may be found in figures 6 and 7.

**Type Soundness** We now have all the pieces necessary to state and prove that execution of a program in our language "can't get stuck." A *stuck program* is a program that is not in the terminal configuration $\texttt{halt}\,i$ and for which no operational rule applies.

**Theorem 4 (Type Soundness)**
*If* $\vdash (S,\iota)$ *and* $(S,\iota) \longmapsto_P^* (S',\iota')$ *then* $(S',\iota')$ *is not stuck.*

The proof itself uses standard Subject Reduction and Progress lemmas in the style popularized by Wright and Felleisen [36] and is mostly mechanical. The proof can be found in Appendix B.

## 6 Related Work

Our type system builds upon the foundational work by other groups on syntactic control of interference [25] and linear type systems in functional programming languages [35, 33, 2]. We also owe much to researchers in alias analysis for imperative languages [12, 15, 7, 9, 26].

Our type system appears most closely related to the shape analysis developed by Sagiv, Reps, and Wilhelm (SRW) [26]. Although the precise relationship is currently unknown to us, it is clear that several of the key features that make SRW shape analysis more effective than similar alias analyses can be expressed in our type system. More specifically:

1. Unlike some other analyses, SRW shape nodes do not contain information about concrete locations or the site where the node was allocated. Our type system drops information about concrete locations using location polymorphism.

2. SRW shape nodes are named with the set of program variables that point to that node. Our type system can only label a node with a single name, but we are able to express the fact that a set of program variables point to that node using the same singleton type for each program variable in the set.

3. SRW shape nodes may be flagged as unshared. Linear types account for unshared shape nodes.

4. A single SRW summary node describes many memory blocks, but through the process of *materialization* a summary node may split off a new, separate shape node. Summary nodes may be represented as recursive types in our framework and materialization can be explained by the process of unrolling and unpacking a recursive and existential type.

$\boxed{\gamma(S) \longmapsto_\gamma S', \theta}$

$$\begin{array}{ll}
\mathtt{union}_{\tau_1 \cup \tau_2}(\ell)(S\{\ell \mapsto v\}) & \longmapsto_\gamma \quad S\{\ell \mapsto \mathtt{union}_{\tau_1 \cup \tau_2}(v)\}, [\,] \\
\mathtt{roll}_\tau(\ell)(S\{\ell \mapsto v\}) & \longmapsto_\gamma \quad S\{\ell \mapsto \mathtt{roll}_\tau(v)\}, [\,] \\
\mathtt{unroll}(\ell)(S\{\ell \mapsto \mathtt{roll}_\tau(v)\}) & \longmapsto_\gamma \quad S\{\ell \mapsto v\}, [\,] \\
\mathtt{pack}_{[c_1,\ldots,c_n|C]\mathtt{as}\,\tau}(\ell)(S\{\ell \mapsto v\}S') & \longmapsto_\gamma \quad S\{\ell \mapsto \mathtt{pack}_{[c_1,\ldots,c_n|S']\mathtt{as}\tau}(v)\}, [\,] \\
\quad \text{where } C = \{\ell_1 \mapsto \tau_1, \ldots, \ell_m \mapsto \tau_m\} \text{ and } S' = \{\ell_1 \mapsto v_1, \ldots, \ell_m \mapsto v_m\} & \\
\mathtt{unpack}\,\ell\,\mathtt{with}\,\Delta\,(S\{\ell \mapsto \mathtt{pack}_{[c_1,\ldots,c_n|S']\mathtt{as}\exists[\Delta|C].\tau}(v)\}) & \longmapsto_\gamma \quad SS'\{\ell \mapsto v\}, [c_1, \ldots, c_n/\Delta]
\end{array}$$

Figure 7: Operational Semantics: Coercions

One of the advantages to our approach is that our language makes it straightforward to create dependencies between functions and data using store or location polymorphism. For example, in our implementation of the Deutsch-Schorr-Waite algorithm, we manipulate continuations that know how to reconstruct a well-formed tree from the current heap structure and we are able to express this dependence in the type system. Explicit manipulation of continuations is necessary in sufficiently low-level typed languages such as Typed Assembly Language when return addresses are interpreted as continuations [21].

Other work has focused on developing expressive pointer logics for describing the shape of the store [20, 13, 27, 3]. Some of these logics can express more sophisticated pointer relationships than the type structure described in this paper. For example, Benedikt *et al.* [3] provide a complex logic that includes path equality and inequality relations, allocation constraints, reachability constraints and other connectives. Our type system is built by starting with the concept of a finite partial map to describe the store and then using a combination of standard type constructors such as singleton, union, polymorphic, existential and recursive types. These type constructors can be reused for a variety of different purposes within a type-preserving compiler from representing closures [19] to data-flow analysis [8] to object encodings [24] to source-level polymorphism and existential types. From an engineering perspective, there are definite advantages to reusing as much type structure as possible.

Several other authors have considered alternatives to pure linear type systems that increase their flexibility. For example, Kobayashi [14] extends standard linear types with data-flow information and Minamide [18] uses a linear type discipline to allow programmers to manipulate "data structures with a hole." Minamide's language allows users to write programs that are compiled into destination-passing style. However, Minamide's language is still quite high-level; he does not show how to verify explicit pointer manipulation. Moreover, neither of these type systems provide the ability to represent cyclic data structures.

Tofte, Talpin, and others [32, 4, 1, 6] have explored the use of region-based memory management. In their work, objects are allocated into one of several *regions* of memory. When a region is deallocated, all the objects in that region are deallocated too. Region-based memory management performs extremely well in many circumstances, but unlike systems based on linear types, space is not, in general, reused on a per-object basis. Moreover, regions cannot be encapsulated inside recursive data structures. However, we believe that some of the techniques we have developed here may be adapted to the region setting and we are eager to investigate a combined framework that can take advantage of both forms of typed memory management.

## Acknowledgements

Fred Smith worked with us on the predecessor to this research and the many stimulating discussions we had together contributed to the current paper. Neal Glew made helpful comments on an earlier draft of this paper.

## References

[1] Alexander Aiken, Manuel Fähndrich, and Raph Levien. Better static memory management: Improving region-based analysis of higher-order languages. In *ACM Conference on Programming Language Design and Implementation*, pages 174–185, La Jolla, California, 1995.

[2] Erik Barendsen and Sjaak Smetsers. Conventional and uniqueness typing in graph rewrite systems (extended abstract). In *Thirteenth Conference on the Foundations of Software Technology and Theoretical Computer Science*, pages 41–51, Bombay, 1993. In Shyamasundar, ed., Springer-Verlag, LNCS 761.

[3] Michael Benedikt, Thomas Reps, and Mooly Sagiv. A decidable logic for describing linked data structures. In *European Symposium on Programming*, pages 2–19, Amsterdam, March 1999.

[4] Lars Birkedal, Mads Tofte, and Magnus Vejlstrup. From region inference to von Neumann machines via region representation inference. In *Twenty-Third ACM Symposium on Principles of Programming Languages*, pages 171–183, St. Petersburg, January 1996.

[5] Perry Cheng and Chris Okasaki. Destination-passing style and generational garbage collection. Unpublished., November 1996.

[6] Karl Crary, David Walker, and Greg Morrisett. Typed memory management in a calculus of capabilities. In *Twenty-Sixth ACM Symposium on Principles of Programming Languages*, pages 262–275, San Antonio, January 1999.

[7] Alain Deutsch. Interprocedural may-alias analysis for pointers: Beyond k-limiting. In *ACM Conference on Programming Language Design and Implementation*, pages 230–241, Orlando, June 1994.

[8] Allyn Dimock, Robert Muller, Franklyn Turbak, and J. B. Wells. Strongly typed flow-directed representation transformations. In *ACM International Conference on Functional Programming*, pages 85–98, Amsterdam, June 1997.

[9] Rakesh Ghiya and Laurie J. Hendren. Is it a tree, a DAG, or a cyclic graph? A shape analysis for heap-directed pointers in C. In *Twenty-Third ACM Symposium on Principles of Programming Languages*, pages 1–15, St. Petersburg Beach, Florida, January 1996.

[10] Dan Grossman and Greg Morrisett. Scalable certification of native code: Experience from compiling to TALx86. Technical Report TR2000-1783, Cornell University, February 2000.

[11] Robert Harper. A simplified account of polymorphic references. *Information Processing Letters*, 51(4):201–206, August 1994.

[12] Neil D. Jones and Steven Muchnick, editors. *Flow analysis and optimization of Lisp-like structures.* Prentice-Hall, 1981.

[13] Nils Klarlund and Michael Schwartzbach. Graph types. In *Twentieth ACM Symposium on Principles of Programming Languages*, pages 196–205, Charleston, January 1993.

[14] Naoki Kobayashi. Quasi-linear types. In *Twenty-Sixth ACM Symposium on Principles of Programming Languages*, pages 29–42, San Antonio, January 1999.

[15] James R. Larus and Paul N. Hilfinger. Detecting conflicts between structure accesses. In *ACM Conference on Programming Language Design and Implementation*, pages 24–31, June 1988.

[16] James Richard Larus. *Restructuring Symbolic Programs for Concurrent Execution on Multiprocessors.* PhD thesis, University of California at Berkeley, May 1989. Available as Berkeley technical report UCB/CSD 89/502.

[17] Erik Meijer, Maarten Fokkinga, and Ross Paterson. Functional programming with bananas, lenses, envelopes, and barbed wire. In *ACM Conference on Functional Programming and Computer Architecture*, 1991. Also published in Lecture Notes in Computer Science, 523, Springer-Verlag.

[18] Y. Minamide. A functional representation of data structures with a hole. In *Twenty-Fifth ACM Symposium on Principles of Programming Languages*, pages 75–84, San Diego, January 1998.

[19] Y. Minamide, G. Morrisett, and R. Harper. Typed closure conversion. In *Twenty-Third ACM Symposium on Principles of Programming Languages*, pages 271–283, St. Petersburg, January 1996.

[20] Bernhard Möller. Towards pointer algebra. *Science of Computer Programming*, 21:57–90, 1993.

[21] Greg Morrisett, Karl Crary, Neal Glew, and David Walker. Stack-based Typed Assembly Language. In *Second International Workshop on Types in Compilation*, pages 95–117, Kyoto, March 1998. Published in Xavier Leroy and Atsushi Ohori, editors, *Lecture Notes in Computer Science*, volume 1473, pages 28-52. Springer-Verlag, 1998.

[22] Greg Morrisett, David Walker, Karl Crary, and Neal Glew. From System F to Typed Assembly Language. In *Twenty-Fifth ACM Symposium on Principles of Programming Languages*, pages 85–97, San Diego, January 1998.

[23] George Necula and Peter Lee. The design and implementation of a certifying compiler. In *ACM Conference on Programming Language Design and Implementation*, pages 333 – 344, Montreal, June 1998.

[24] Benjamin Pierce and David Turner. Simple type-theoretic foundations for object-oriented programming. *Journal of functional programming*, 4:207–247, 1994.

[25] John C. Reynolds. Syntactic control of interference. In *Fifth ACM Symposium on Principles of Programming Languages*, pages 39–46, Tucson, 1978.

[26] Mooly Sagiv, Thomas Reps, and Reinhard Wilhelm. Solving shape-analysis problems in languages with destructive updating. *ACM Transactions on Programming Languages and Systems*, 20(1):1–50, January 1998.

[27] Mooly Sagiv, Thomas Reps, and Reinhard Wilhelm. Parametric shape analysis via 3-valued logic. In *Twenty-Sixth ACM Symposium on Principles of Programming Languages*, pages 105–118, San Antonio, January 1999.

[28] H. Schorr and W. M. Waite. An efficient machine-independent procedure for garbage collection in various list structures. *Communications of the ACM*, 10(8):501–506, August 1967.

[29] Frederick Smith, David Walker, and Greg Morrisett. Alias types. In *European Symposium on Programming*, March 2000. To appear. Available at http://www.cs.cornell.edu/talc/papers.html.

[30] Johnathan Sobel and Daniel Friedman. Recycling continuations. In *ACM International Conference on Functional Programming*, pages 251–260, Baltimore, September 1998.

[31] TALx86. See http://www.cs.cornell.edu/talc for an implementation of Typed Assembly Language based on Intel's IA32 architecture.

[32] Mads Tofte and Jean-Pierre Talpin. Implementation of the typed call-by-value λ-calculus using a stack of regions. In *Twenty-First ACM Symposium on Principles of Programming Languages*, pages 188–201, Portland, Oregon, January 1994.

[33] David N. Turner, Philip Wadler, and Christian Mossin. Once upon a type. In *ACM International Conference on Functional Programming and Computer Architecture*, San Diego, CA, June 1995.

[34] Philip Wadler. *Listlessness is Better than Laziness.* PhD thesis, Carnegie Mellon University, August 1985. Available as Carnegie Mellon University technical report CMU-CS-85-171.

[35] Philip Wadler. Linear types can change the world! In M. Broy and C. Jones, editors, *Progarmming Concepts and Methods*, Sea of Galilee, Israel, April 1990. North Holland. IFIP TC 2 Working Conference.

[36] Andrew K. Wright and Matthias Felleisen. A syntactic approach to type soundness. *Information and Computation*, 115(1):38–94, 1994.

## A Type Well-formedness

$\boxed{\Delta \vdash c : \kappa}$

$$\frac{}{\Delta \vdash \ell : \texttt{Loc}} \qquad \frac{}{\Delta \vdash \rho : \Delta(\rho)}$$

$$\frac{}{\Delta \vdash \emptyset : \texttt{Store}} \qquad \frac{\Delta \vdash C : \texttt{Store} \quad \Delta \vdash \eta : \texttt{Loc} \quad \Delta \vdash \tau : \texttt{Type}}{\Delta \vdash C \otimes \{\eta \mapsto \tau\} : \texttt{Store}}$$

$$\frac{}{\Delta \vdash \epsilon : \Delta(\epsilon)} \qquad \frac{\Delta \vdash C : \texttt{Store} \quad \Delta \vdash \epsilon : \texttt{Store}}{\Delta \vdash C \otimes \epsilon : \texttt{Store}}$$

$$\frac{}{\Delta \vdash \alpha : \Delta(\alpha)} \qquad \frac{\Delta \vdash \sigma : \texttt{Small}}{\Delta \vdash \sigma : \texttt{Type}}$$

$$\frac{\Delta \vdash \sigma_1 : \texttt{Small} \quad \cdots \quad \Delta \vdash \sigma_n : \texttt{Small}}{\Delta \vdash \langle \sigma_1, \ldots, \sigma_n \rangle : \texttt{Type}}$$

$$\frac{\Delta \vdash \tau_1 : \texttt{Type} \quad \Delta \vdash \tau_2 : \texttt{Type}}{\Delta \vdash \tau_1 \cup \tau_2 : \texttt{Type}}$$

$$\frac{\Delta,\Delta' \vdash C : \mathtt{Store} \qquad \Delta,\Delta' \vdash \tau : \mathtt{Type} \quad (\mathit{Dom}(\Delta) \cap \mathit{Dom}(\Delta') = \emptyset)}{\Delta \vdash \exists[\Delta' \mid C].\tau : \mathtt{Type}}$$

$$\frac{\Delta, \alpha{:}(\kappa_1,\ldots,\kappa_n) \to \mathtt{Type}, \beta_1{:}\kappa_1,\ldots,\beta_n{:}\kappa_n \vdash \tau : \mathtt{Type} \quad (\text{for } 1 \le i \le n.\beta_i \notin \mathit{Dom}(\Delta))}{\Delta \vdash \mathtt{rec}\,\alpha\,(\beta_1{:}\kappa_1,\ldots,\beta_n{:}\kappa_n).\tau : (\kappa_1,\ldots,\kappa_n) \to \mathtt{Type}}$$

$$\frac{\Delta \vdash c : (\kappa_1,\ldots,\kappa_n) \to \mathtt{Type} \quad \Delta \vdash c_1 : \kappa_1 \quad \cdots \quad \Delta \vdash c_n : \kappa_n}{\Delta \vdash c\,(c_1,\ldots,c_n) : \mathtt{Type}}$$

$$\frac{}{\Delta \vdash \mathit{int} : \mathtt{Small}} \qquad \frac{}{\Delta \vdash \mathcal{S}(i) : \mathtt{Small}} \qquad \frac{\Delta \vdash \eta : \mathtt{Loc}}{\Delta \vdash \mathit{ptr}(\eta) : \mathtt{Small}}$$

$$\frac{\Delta,\Delta' \vdash C : \mathtt{Store} \quad \Delta,\Delta' \vdash \sigma_1 : \mathtt{Small} \quad \cdots \quad \Delta,\Delta' \vdash \sigma_n : \mathtt{Small} \quad (\mathit{Dom}(\Delta) \cap \mathit{Dom}(\Delta') = \emptyset)}{\Delta \vdash \forall[\Delta' \mid C].(\sigma_1,\ldots,\sigma_n) \to \mathbf{0} : \mathtt{Small}}$$

$\boxed{\Delta \vdash a_1 = a_2 : \mathtt{Atom}}$

$$\frac{\Delta \vdash \eta : \mathtt{Loc} \quad \Delta \vdash \tau = \tau' : \mathtt{Type}}{\Delta \vdash \{\eta \mapsto \tau\} = \{\eta \mapsto \tau'\} : \mathtt{Atom}}$$

$$\frac{\Delta \vdash \epsilon : \mathtt{Store}}{\Delta \vdash \epsilon = \epsilon : \mathtt{Atom}}$$

$\boxed{\Delta \vdash c_1 = c_2 : \kappa}$

$$\frac{\Delta \vdash a_1 = a_1'' : \mathtt{Atom} \quad \cdots \quad \Delta \vdash a_n = a_n'' : \mathtt{Atom} \quad a_1',\ldots,a_n' \text{ is a permutation of } a_1'',\ldots,a_n''}{\Delta \vdash \emptyset \otimes a_1 \otimes \cdots \otimes a_n = \emptyset \otimes a_1' \otimes \cdots \otimes a_n' : \mathtt{Store}}$$

Add all congruence rules.

## B Type Soundness

**Lemma 5** *If $\Delta \vdash c : \kappa$ then $\mathrm{FV}(c) \subseteq \mathit{Dom}(\Delta)$.*

**Proof:** By induction on the kinding and equality derivations.

**Lemma 6 (Properties of Type Equality)**

1. *(Well-formedness) If $\Delta \vdash c_1 = c_2 : \kappa$ then $\Delta \vdash c_1 : \kappa$ and $\Delta \vdash c_2 : \kappa$.*
2. *(Symmetry) If $\Delta \vdash c_1 = c_2 : \kappa$ then $\Delta \vdash c_2 = c_1 : \kappa$*
3. *(Transitivity) If $\Delta \vdash c_1 = c_2 : \kappa$ and $\Delta \vdash c_2 = c_3 : \kappa$ then $\Delta \vdash c_1 = c_3 : \kappa$*

**Proof:** By induction on the equality derivation.

**Lemma 7** *If $\Delta \vdash c : \kappa$ and $\alpha \notin \mathit{Dom}(\Delta)$ then $\Delta, \alpha{:}\kappa' \vdash c : \kappa$*

**Proof:** By induction on the kinding derivation.

**Lemma 8 (Type Substitution)** *If $\cdot \vdash c : \kappa$ and $\theta = [c/\alpha]$ then*

1. *if $\Delta, \alpha{:}\kappa, \Delta'; \Gamma \vdash v : \tau$ then $\Delta, \Delta'; \theta(\Gamma) \vdash \theta(v) : \theta(\tau)$.*
2. *if $\Delta, \alpha{:}\kappa, \Delta'; C; \Gamma \vdash \iota$ then $\Delta, \Delta'; \theta(C); \theta(\Gamma) \vdash \theta(\iota)$*

**Proof:** By induction on the typing derivation.

**Lemma 9 (Value Substitution)** *If $\cdot;\cdot \vdash v : \tau$ and $\theta = [v/x]$ then*

1. *if $\Delta; \Gamma, x{:}\tau, \Gamma' \vdash v' : \tau'$ then $\Delta; \Gamma, \Gamma' \vdash \theta(v') : \tau'$*
2. *if $\Delta; C; \Gamma, x{:}\tau, \Gamma' \vdash \iota$ then $\Delta; C; \Gamma, \Gamma' \vdash \theta(\iota)$*

**Proof:** By induction on the typing derivation.

**Lemma 10** *If for all $x \in \mathit{Dom}(\Gamma)$, $\Delta \vdash \Gamma(x) : \mathtt{Small}$ and $\Delta; \Gamma \vdash v : \tau$ and $\Delta; \Gamma \vdash v : \tau'$ then $\Delta \vdash \tau = \tau' : \mathtt{Type}$*

**Proof:** By induction on the typing derivation.

**Lemma 11** *If for all $x \in \mathit{Dom}(\Gamma), \Delta \vdash \Gamma(x) = \Gamma'(x) : \mathtt{Small}$ and $\Delta \vdash C = C' : \mathtt{Store}$ then*

1. *if $\Delta; \Gamma \vdash v : \tau$ then $\Delta; \Gamma' \vdash v : \tau$*
2. *if $\Delta; C; \Gamma \vdash \iota$ then $\Delta; C'; \Gamma' \vdash \iota$*

**Proof:** By induction on the typing derivation.

**Lemma 12 (Canonical Value Forms)** *If $\cdot;\cdot \vdash v : \tau$ then*

1. *if $\tau = \mathit{int}$ then $v = i$.*
2. *if $\tau = \mathcal{S}(i)$ then $v = \mathcal{S}(i)$*
3. *if $\tau = \mathit{ptr}(\ell)$ then $v = \mathtt{ptr}(\ell)$*
4. *if $\tau = \langle \sigma_1,\ldots,\sigma_n \rangle$ then*
   (a) $v = \langle v_1,\ldots,v_n \rangle$
   (b) $\cdot;\cdot \vdash v_i : \sigma_i$
5. *if $\tau = \tau_1 \cup \tau_2$ then*
   (a) $v = \mathtt{union}_{\tau_1' \cup \tau_2'}(v')$
   (b) $\cdot;\cdot \vdash v' : \tau_i$ *where* $i = 1$ *or* $2$
   (c) $\cdot \vdash \tau_1 = \tau_1' : \mathtt{Type}$
   (d) $\cdot \vdash \tau_2 = \tau_2' : \mathtt{Type}$
6. *if $\tau = \mathtt{rec}\,\alpha\,(\Delta).\tau'\,(c_1,\ldots,c_n)$ then*
   (a) $v = \mathtt{roll}_{\tau''}(v')$
   (b) $\cdot;\cdot \vdash v' : \tau'[\mathtt{rec}\,\alpha\,(\Delta).\tau'/\alpha][c_1,\ldots,c_n/\Delta]$
   (c) $\cdot \vdash \tau = \tau'' : \mathtt{Type}$
7. *if $\tau = \exists[\Delta \mid C].\tau'$ then*
   (a) $v = \mathtt{pack}_{[c_1,\ldots,c_n|S]\mathtt{as}\tau''}(v')$
   (b) $\cdot \vdash \tau = \tau'' : \mathtt{Type}$
   (c) $\Delta = \alpha_1{:}\kappa_1,\ldots,\alpha_n{:}\kappa_n$
   (d) *for* $1 \le i \le n$, $\cdot \vdash c_i : \kappa_i$
   (e) $\cdot;\cdot \vdash v' : \tau'[c_1,\ldots,c_n/\Delta]$
   (f) $\vdash S : C[c_1,\ldots,c_n/\Delta]$
8. *if $\tau = \forall[\Delta \mid C].(\sigma_1,\ldots,\sigma_n) \to \mathbf{0}$ then*
   (a) $v = v'[c_1',\ldots,c_n']$ *and* $v' = \mathtt{fix}\,f[\Delta',\Delta \mid C''](x_1{:}\sigma_1',\ldots,x_n{:}\sigma_n').\iota$
   (b) $\Delta' = \alpha_1{:}\kappa_1,\ldots,\alpha_n{:}\kappa_n$
   (c) *for* $1 \le i \le n$, $\cdot \vdash c_i' : \kappa_i$
   (d) $\cdot \vdash \mathtt{fix}\,f[\Delta',\Delta \mid C](x_1{:}\sigma_1,\ldots,x_n{:}\sigma_n).\iota : \tau$
   (e) $\cdot \vdash (\forall[\Delta \mid C''].(\sigma_1',\ldots,\sigma_n') \to \mathbf{0})[c_1,\ldots,c_n/\Delta'] = (\forall[\Delta \mid C].(\sigma_1,\ldots,\sigma_n) \to \mathbf{0}) :$

**Proof:** By induction on the typing derivation.

**Lemma 13 (Canonical Store Forms)** *If $\vdash S : C$ and $\cdot \vdash C = C' \otimes \{\ell \mapsto \tau\} : \mathtt{Store}$ then*

1. $S = S'\{\ell \mapsto v\}$
2. $\vdash S' : C'$
3. $\cdot;\cdot \vdash v : \tau$

**Proof:**

The typing derivation $\vdash S : C$ has the form

$$\frac{\begin{array}{c} S = \{\ell_1 \mapsto v_1, \ldots, \ell_n \mapsto v_n\} \\ \cdot \vdash C = \{\ell_1 \mapsto \tau_1, \ldots, \ell_n \mapsto \tau_n\} : \texttt{Store} \\ \cdot; \cdot \vdash v_i : \tau_i \qquad (\text{for } 1 \leq i \leq n) \end{array}}{\vdash S : C}$$

By Lemma 6 and Lemma 5, $C'$ can contain no free variables and therefore may be written $\{\ell'_1 \mapsto v'_1, \ldots, \ell'_k \mapsto v'_k\}$. By transitivity of equality,

$$\cdot \vdash \{\ell'_1 \mapsto \tau'_1, \ldots, \ell'_k \mapsto \tau'_k, \ell \mapsto \tau\} = \{\ell_1 \mapsto \tau_1, \ldots, \ell_n \mapsto \tau_n\} : \texttt{Store}$$

By inspection of the definition of constructor equality, we know that

1. for $1 \leq i \leq k$, $\cdot \vdash \tau'_i = \tau''_i : \texttt{Type}$ and
2. $\cdot \vdash \tau = \tau'' : \texttt{Type}$ and
3. $\ell'_1 \mapsto \tau''_1, \ldots, \ell'_k \mapsto \tau''_k, \ell \mapsto \tau''$ is a permutation of $\ell_1 \mapsto \tau_1, \ldots, \ell_n \mapsto \tau_n$

In order for the two sequences to be permutations of one another $k$ must be $n-1$. Moreover, for some $i$, $\ell_i \mapsto \tau_i$ must be $\ell \mapsto \tau''$ and without loss of generality, we will assume that $i$ is $n$. Therefore, $\ell'_1 \mapsto \tau''_1, \ldots, \ell'_k \mapsto \tau''_k$ is a permutation of $\ell_1 \mapsto \tau_1, \ldots, \ell_{n-1} \mapsto \tau_{n-1}$. Consequently,

$$\cdot \vdash C' = \{\ell_1 \mapsto \tau_1, \ldots, \ell_{n-1} \mapsto \tau_{n-1}\} : \texttt{Store}$$

Let $S'$ be $\{\ell_1 \mapsto v_1, \ldots, \ell_{n-1} \mapsto v_{n-1}\}$ and let $v$ be $v_n$. We have $S = S'\{\ell \mapsto v\}$. We can also conclude from the judgement $\vdash C : S$ that for $1 \leq i \leq n-1$, $\cdot; \cdot \vdash v_i : \tau_i$. Therefore, we have

$$\frac{\begin{array}{c} S' = \{\ell_1 \mapsto v_1, \ldots, \ell_{n-1} \mapsto v_{n-1}\} \\ \cdot \vdash C' = \{\ell_1 \mapsto \tau_1, \ldots, \ell_{n-1} \mapsto \tau_{n-1}\} : \texttt{Store} \\ \cdot; \cdot \vdash v_i : \tau_i \qquad (\text{for } 1 \leq i \leq n-1) \end{array}}{\vdash S' : C'}$$

From the judgement $\vdash S : C$, we also know that $\cdot; \cdot \vdash v_n : \tau_n$ and since $v$ is $v_n$ and $\tau$ is $\tau_n$, we have $\cdot; \cdot \vdash v : \tau$.

□

**Lemma 14** *If* $\vdash S'\{\ell \mapsto v\} : C$ *and* $\cdot \vdash C = C' \otimes \{\ell \mapsto \tau\} : \texttt{Store}$ *then*

1. $\vdash S' : C'$
2. $\cdot; \cdot \vdash v : \tau$

**Proof:** Corollary of Canonical Store Forms.

**Lemma 15** *If*

1. $\vdash S'\{\ell \mapsto v\} : C$
2. $\cdot \vdash C = C' \otimes \{\ell \mapsto \tau\} : \texttt{Store}$
3. $\cdot; \cdot \vdash v' : \tau'$

*then* $\vdash S'\{\ell \mapsto v'\} : C' \otimes \{\ell \mapsto \tau'\}$

**Proof:**

By (1), (2), and Lemma 14, $\vdash S' : C'$. Hence, by (3) and inspection of the store typing judgement, $\vdash S'\{\ell \mapsto v'\} : C' \otimes \{\ell \mapsto \tau'\}$

□

**Lemma 16** *If* $Dom(S) \cap Dom(S') = \emptyset$ *and* $\vdash S : C$ *and* $\vdash S' : C'$ *then* $\vdash SS' : C@C'$

**Proof:**

Since $Dom(S) \cap Dom(S') = \emptyset$, we know that $SS'$ is a store. Inspection of the store typing judgement and examination of the definition of equality provides the result.

□

**Lemma 17**

1. *If* $\Delta; \Gamma \vdash v : \sigma$ *then* $\texttt{L}(v) = 0$.
2. *If* $\Delta; C; \Gamma \vdash \iota$ *then* $\texttt{L}(\iota) = 0$.

**Proof:** By induction on the typing derivations.

**Lemma 18 (Preservation)** *If* $\vdash (S, \iota)$ *and* $(S, \iota) \longmapsto_P (S', \iota')$ *then* $\vdash (S', \iota')$

**Proof:**

By cases on the operational rule that applied.

- Operational Rule:

  $$(S, \texttt{new}\ \rho, x, i; \iota) \longmapsto_P (S\{\ell \mapsto v\}, \iota[\ell/\rho][\texttt{ptr}(\ell)/x])$$

  where $\ell \notin S, \iota$ and $v = \overbrace{\langle \mathcal{S}(0), \ldots, \mathcal{S}(0) \rangle}^{i}$

  Typing Assumption:

  1. $\texttt{GU}(S)$
  2. $\vdash S : C$.
  3. $\cdot; C; \cdot \vdash \texttt{new}\ \rho, x, i; \iota$.

  First, we know $\texttt{GU}(S\{\ell \mapsto v\})$ since $\texttt{GU}(S)$ and $\ell \notin S$.
  Second, we can conclude:

  $$\cdot; \cdot \vdash v : \overbrace{\langle \mathcal{S}(0), \ldots, \mathcal{S}(0) \rangle}^{i}$$

  Consequently, by inspection of the store typing judgement,

  $$\vdash S\{\ell \mapsto v\} : C \otimes \{\ell \mapsto \overbrace{\langle \mathcal{S}(0), \ldots, \mathcal{S}(0) \rangle}^{i}\}$$

  Third, the premise of the instruction typing judgement is

  $$\rho{:}\texttt{Loc}; C \otimes \{\rho \mapsto \overbrace{\langle \mathcal{S}(0), \ldots, \mathcal{S}(0) \rangle}^{i}\}; x{:}ptr(\rho) \vdash \iota$$

  By Type and Value Substitution Lemmas,

  $$\cdot; C \otimes \{\ell \mapsto \overbrace{\langle \mathcal{S}(0), \ldots, \mathcal{S}(0) \rangle}^{i}\}; \cdot \vdash \iota[\ell/\rho][ptr(\ell)/x]$$

  Consequently, $\vdash (S\{\ell \mapsto v\}, \iota[\ell/\rho][\texttt{ptr}(\ell)/x])$

- Operational Rule:

  $$(S\{\ell \mapsto \langle v_1, \ldots, v_n \rangle\}, \texttt{free}\ \texttt{ptr}(\ell); \iota) \longmapsto_P (S, \iota)$$

  Typing Assumption:

  1. $\texttt{GU}(S\{\ell \mapsto \langle v_1, \ldots, v_n \rangle\})$
  2. $\vdash S\{\ell \mapsto \langle v_1, \ldots, v_n \rangle\} : C$.
  3. $\cdot; C; \cdot \vdash \texttt{free}\ \texttt{ptr}(\ell); \iota$.

  From 1, we have $\texttt{GU}(S)$.
  The instruction judgement 3 must have the form:

  $$\frac{\begin{array}{c} \cdot; \cdot \vdash v : ptr(\ell) \\ \cdot \vdash C = C' \otimes \{\ell \mapsto \langle \sigma_1, \ldots, \sigma_n \rangle\} : \texttt{Store} \\ \cdot; C'; \cdot \vdash \iota \end{array}}{\cdot; C; \cdot \vdash \texttt{free}\ v; \iota}$$

  Hence, by Lemma 14, we can deduce that $\vdash S : C'$.
  Moreover, we have $\cdot; C'; \cdot \vdash \iota$ directly.
  Therefore, $\vdash (S, \iota)$.

- Operational Rule:

$$(S\{\ell \mapsto \langle v_1,\ldots,v_n\rangle\}, \texttt{let}\ x = (\texttt{ptr}(\ell)).i;\iota) \longmapsto_P \\ (S\{\ell \mapsto \langle v_1,\ldots,v_n\rangle\}, \iota[v_i/x])$$

where $1 \leq i \leq n$

Typing Assumption:

1. $\texttt{GU}(S\{\ell \mapsto \langle v_1,\ldots,v_n\rangle\})$
2. $\vdash S\{\ell \mapsto \langle v_1,\ldots,v_n\rangle\} : C$.
3. $\cdot;C;\cdot \vdash \texttt{let}\ x = (\texttt{ptr}(\ell)).i;\iota$.

Where the instruction derivation has the following form:

$$\frac{\begin{array}{c}\cdot;\cdot \vdash \texttt{ptr}(\ell) : ptr(\ell) \\ \cdot \vdash C = C' \otimes \{\ell \mapsto \langle \sigma_1,\ldots,\sigma_n\rangle\} : \texttt{Store} \\ \cdot;C;x{:}\sigma_i \vdash \iota\end{array}}{\cdot;C;\cdot \vdash \texttt{let}\ x = (\texttt{ptr}(\ell)).i;\iota}$$

The instruction derivation contains the fact $\cdot;C;x{:}\sigma_i \vdash \iota$ and by Lemma 14, we can conclude that $\cdot;\cdot \vdash \langle v_1,\ldots,v_n\rangle : \langle \sigma_1,\ldots,\sigma_n\rangle$. By Canonical Forms, we can conclude that $\cdot;\cdot \vdash v_i : \sigma_i$. Hence, from the Value Substitution Lemma, we know that $\cdot;C;\cdot \vdash \iota[v_i/x]$. From this judgement and (1) and (2), we can conclude $\vdash (S\{\ell \mapsto \langle v_1,\ldots,v_n\rangle\}, \iota[v_i/x])$

- Operational Rule:

$$(S\{\ell \mapsto \langle v_1,\ldots,v_i,\ldots,v_n\rangle\}, (\texttt{ptr}(\ell)).i := v';\iota) \longmapsto_P \\ (S\{\ell \mapsto \langle v_1,\ldots,v',\ldots,v_n\rangle\}, \iota)$$

Typing Assumption:

1. $\texttt{GU}(S\{\ell \mapsto \langle v_1,\ldots,v_i,\ldots,v_n\rangle\})$
2. $\vdash S\{\ell \mapsto \langle v_1,\ldots,v_i,\ldots,v_n\rangle\} : C$.
3. $\cdot;C;\cdot \vdash (\texttt{ptr}(\ell)).i := v';\iota$.

The instruction typing judgement has the form:

$$\frac{\begin{array}{c}\cdot;\cdot \vdash \texttt{ptr}(\ell) : ptr(\ell) \\ \cdot;\cdot \vdash v' : \sigma \\ \cdot \vdash C = C' \otimes \{\ell \mapsto \langle \sigma_1,\ldots,\sigma_i,\ldots,\sigma_n\rangle\} : \texttt{Store} \\ \cdot;C' \otimes \{\ell \mapsto \langle \sigma_1,\ldots,\sigma,\ldots,\sigma_n\rangle\};\cdot \vdash \iota\end{array}}{\cdot \vdash (\texttt{ptr}(\ell)).i := v';\iota}$$

By Lemma 14 we can conclude that

$$\cdot;\cdot \vdash \langle v_1,\ldots,v_n\rangle : \langle \sigma_1,\ldots,\sigma_n\rangle$$

By Canonical Value Forms, we can deduce that (4) for all $1 \leq i \leq n$

$$\cdot;\cdot \vdash v_j : \sigma_j$$

From the instruction typing judgement, we also have the fact that (5)

$$\cdot;\cdot \vdash v' : \sigma$$

By Lemma 17, $\texttt{L}(v_i) = \texttt{L}(v') = 0$. Consequently, since $\texttt{GU}(S\{\ell \mapsto \langle v_1,\ldots,v_i,\ldots,v_n\rangle\})$, we know (6)

$$\texttt{GU}(S\{\ell \mapsto \langle v_1,\ldots,v',\ldots,v_n\rangle\})$$

By Lemma 14 we can also conclude that $\vdash S : C'$. From (4), (5), and the typing rule for tuples, we can conclude that (7)

$$\cdot;\cdot \vdash \langle v_1,\ldots,v',\ldots,v_n\rangle : \langle \sigma_1,\ldots,\sigma,\ldots,\sigma_n\rangle$$

Therefore, from (2), (7), and the constraint equality judgement from the instruction typing judgement, we can conclude by Lemma 15 that

$$\vdash S\{\ell \mapsto \langle v_1,\ldots,v',\ldots,v_n\rangle\} : \\ C' \otimes \{\ell \mapsto \langle \sigma_1,\ldots,\sigma,\ldots,\sigma_n\rangle\}$$

These facts and the instruction typing judgement imply that $\vdash (S\{\ell \mapsto \langle v_1,\ldots,v',\ldots,v_n\rangle\}, \iota)$

- Operational Rule

$$(S\{\ell \mapsto v\}, \texttt{case}\,\texttt{ptr}(\ell)\,(\texttt{inl} \Rightarrow \iota_1 \mid \texttt{inr} \Rightarrow \iota_2)) \longmapsto_P \\ (S\{\ell \mapsto v'\}, \iota_i)$$

where

$$\begin{array}{rcl} i & = & 1 \text{ or } 2 \\ v & = & \texttt{union}_{\tau_1 \cup \tau_2}(v') \\ v' & = & \varsigma_1(\cdots\varsigma_m(\langle \mathcal{S}(i), v_1,\ldots,v_n\rangle)\cdots) \end{array}$$

Typing Assumption:

1. $\texttt{GU}(S\{\ell \mapsto v\})$
2. $\vdash S\{\ell \mapsto v\} : C$.
3. $\cdot;C;\cdot \vdash \texttt{case}\,\texttt{ptr}(\ell)\,(\texttt{inl} \Rightarrow \iota_1 \mid \texttt{inr} \Rightarrow \iota_2)$.

Where the instruction typing judgement has the form:

$$\frac{\begin{array}{c}\cdot \vdash \texttt{ptr}(\ell) : ptr(\ell) \\ \cdot \vdash C = C' \otimes \{\ell \mapsto \tau_1 \cup \tau_2\} : \texttt{Store} \\ \cdot \vdash \tau_1 = \tau_1' : \texttt{Type} \\ \cdot \vdash \tau_2 = \tau_2' : \texttt{Type} \\ \cdot;C' \otimes \{\ell \mapsto \tau_1\};\cdot \vdash \iota_1 \\ \cdot;C' \otimes \{\ell \mapsto \tau_2\};\cdot \vdash \iota_2\end{array}}{\cdot;C;\cdot \vdash \texttt{case}\,\texttt{ptr}(\ell)\,(\texttt{inl} \Rightarrow \iota_1 \mid \texttt{inr} \Rightarrow \iota_2)}$$

Where $\tau_1'$ is

$$\exists[\Delta_1' \mid C_1'].\cdots\exists[\Delta_j' \mid C_j'].\langle \mathcal{S}(1), \sigma_1',\ldots,\sigma_k'\rangle$$

and $\tau_2'$ is

$$\exists[\Delta_1'' \mid C_1''].\cdots\exists[\Delta_m'' \mid C_m''].\langle \mathcal{S}(2), \sigma_1'',\ldots,\sigma_n''\rangle$$

First, by inspection of the definition of $\texttt{L}(\cdot)$, we can conclude that $\texttt{L}(v') = \texttt{L}(v)$ and therefore that $\texttt{L}(S\{\ell \mapsto v'\}) = \texttt{L}(S\{\ell \mapsto v\})$. Since $\texttt{GU}(S\{\ell \mapsto v\})$ we can conclude $\texttt{GU}(S\{\ell \mapsto v'\})$.

Second, from (2) and by Canonical Store Forms and Canonical Value Forms, we can conclude that

$$\cdot;\cdot \vdash v' : \tau_i$$

Hence, by Lemma 15, we can deduce that

$$\vdash S\{\ell \mapsto v'\} : C' \otimes \{\ell \mapsto \tau_i\}$$

From the instruction typing judgement, we have

$$\cdot;C' \otimes \{\ell \mapsto \tau_i\};\cdot \vdash \iota_i$$

Therefore, we can conclude that $\vdash (S\{\ell \mapsto v'\}, \iota_i)$.

- Operational Rule

$$(S, v(v_1,\ldots,v_n)) \longmapsto_P (S, \theta(\iota))$$

where

$$\begin{array}{rcl} v & = & v'[c_1,\ldots,c_m] \\ v' & = & \texttt{fix}f[\Delta \mid C](x_1{:}\sigma_1,\ldots,x_n{:}\sigma_n).\iota \\ \theta & = & [c_1,\ldots,c_m/\Delta][v'/f][v_1,\ldots,v_n/x_1,\ldots,x_n] \\ \Delta & = & \beta_1{:}\kappa_1,\ldots,\beta_m{:}\kappa_m \end{array}$$

Typing Assumption:

1. $\texttt{GU}(S)$
2. $\vdash S : C$.
3. $\cdot;C;\cdot \vdash v(v_1,\ldots,v_n)$.

Where the instruction typing judgement has the form:

$$\frac{\begin{array}{c}\cdot;\cdot \vdash v : \forall[\cdot \mid C].(\sigma_1,\ldots,\sigma_n) \to \mathbf{0} \\ \cdot;\cdot \vdash v_1 : \sigma_1 \quad \cdots \quad \cdot;\cdot \vdash v_n : \sigma_n\end{array}}{\cdot;C;\cdot \vdash v(v_1,\ldots,v_n)}$$

By Canonical Value Forms,

$$\Delta; C'; f{:}\forall[\Delta \mid C'].(\sigma_1',\ldots,\sigma_n') \to \mathbf{0}, x_1{:}\sigma_1',\ldots,x_n{:}\sigma_n' \vdash \iota$$

and
$$\begin{array}{c}\cdot \vdash \theta(\forall[\cdot \mid C'].(\sigma_1',\ldots,\sigma_n') \to \mathbf{0}) = \\ \forall[\cdot \mid C].(\sigma_1,\ldots,\sigma_n) \to \mathbf{0} : \mathtt{Small}\end{array}$$

By definition of equality $\cdot \vdash \theta(C') = C : \mathtt{Store}$ and also, for $1 \le i \le m$,
$$\cdot \vdash c_i : \kappa_i$$
From the instruction typing judgement, each value $v_i$ is well-formed with type $\sigma_i$. Consequently, by Type and Value Substitution, we know that

$$\cdot;\theta(C');\cdot \vdash \theta(\iota)$$

By Lemma 11 and the fact that $\cdot \vdash \theta(C') = C : \mathtt{Store}$, we have
$$\cdot;C;\cdot \vdash \theta(\iota)$$
From this fact (1) and (2), we can conclude $\vdash (S, \theta(\iota))$.

- Operational Rule

$$(S, \mathtt{coerce}(\gamma); \iota) \longmapsto_P (S', \theta(\iota))$$

where $\gamma(S) \longmapsto_\gamma S', \theta$ and $\gamma = \mathtt{union}_{\tau_1 \cup \tau_2}(\ell)$ or $\mathtt{roll}_\tau(\ell)$ or $\mathtt{unroll}(\ell)$ is similar to the case for the instruction $(v).i := v'$.

- Operational Rule

$$\begin{array}{c}(S\{\ell \mapsto v\}, \mathtt{coerce}(\gamma); \iota) \longmapsto_P \\ (SS'\{\ell \mapsto v'\}, \theta(\iota))\end{array}$$

where

$$\begin{array}{rcl} v & = & \mathtt{pack}_{[c_1,\ldots,c_n \mid S']\mathtt{as}\exists[\Delta \mid C].\tau}(v') \\ \gamma & = & \mathtt{unpack}\,\ell\,\mathtt{with}\,\Delta \\ \theta & = & [c_1,\ldots,c_n/\Delta] \\ \Delta & = & \beta_1{:}\kappa_1,\ldots,\beta_n{:}\kappa_n \end{array}$$

Typing Assumption:

1. $\mathtt{GU}(S\{\ell \mapsto v\})$
2. $\vdash S\{\ell \mapsto v\} : C$.
3. $\cdot;C;\cdot \vdash \mathtt{coerce}(\gamma);\iota$.

Where the coercion typing judgement is

$$\frac{\cdot \vdash C = C'' \otimes \{\ell \mapsto \exists[\Delta \mid C'].\tau\} : \mathtt{Store}}{\cdot;C \vdash \mathtt{unpack}\,\ell\,\mathtt{with}\,\Delta \implies \Delta; C'' \otimes \{\ell \mapsto \tau\}@C'}$$

and the instruction typing judgement implies $\iota$ is well-formed:

$$\Delta; C'' \otimes \{\ell \mapsto \tau\} \otimes C'; \cdot \vdash \iota$$

By inspection of the definition of $\mathtt{L}(\cdot)$, we can deduce that $\mathtt{L}(S\{\ell \mapsto v\}) = \mathtt{L}(SS'\{\ell \mapsto v'\})$ Therefore, since $\mathtt{GU}(S\{\ell \mapsto v\})$, we can conclude that $\mathtt{GU}(SS'\{\ell \mapsto v'\})$.
By (2), the coercion typing judgement and Lemma 14 we can deduce that $\cdot \vdash v : \exists[\Delta \mid C'].\tau$. Consequently, by Canonical Value Forms, we can conclude that $\cdot;\cdot \vdash v' : \theta(\tau)$. From this fact, (2), and the equality from the coercion typing judgement, using Lemma 15, we can conclude that

$$\vdash S\{\ell \mapsto v'\} : C'' \otimes \{\ell \mapsto \theta(\tau)\}$$

By Canonical Value forms, we also know that

$$\vdash S' : \theta(C')$$

Therefore, by Lemma 16 we can conclude that

$$\vdash S\{\ell \mapsto v'\}S' : C'' \otimes \{\ell \mapsto \theta(\tau)\}@\theta(C')$$

Hence the equivalent store is also well-formed:

$$\vdash SS'\{\ell \mapsto v'\} : C'' \otimes \{\ell \mapsto \theta(\tau)\}@\theta(C')$$

Canonical Value Forms also implies that for $1 \le i \le n$,

$$\cdot \vdash c_i : \kappa_i$$

Now using the instruction typing judgement and the Type Substitution Lemma we can deduce that

$$\cdot; C'' \otimes \{\ell \mapsto \theta(\tau)\}@\theta(C'); \cdot \vdash \theta(\iota)$$

Consequently, $\vdash (SS'\{\ell \mapsto v'\}, \theta(\iota))$.

- Operational Rule:

$$(SS'\{\ell \mapsto v\}, \mathtt{coerce}(\gamma); \iota) \longmapsto_P (S\{\ell \mapsto v'\}, \iota)$$

where

$$\begin{array}{rcl} v' & = & \mathtt{pack}_{[c_1,\ldots,c_n \mid S']\mathtt{as}\exists[\Delta \mid C'].\tau}(v) \\ \gamma & = & \mathtt{pack}_{[c_1,\ldots,c_n \mid \theta(C')]\mathtt{as}\ \exists[\Delta \mid C'].\tau}(\ell) \\ \theta & = & [c_1,\ldots,c_n/\Delta] \\ S' & = & \{\ell_1 \mapsto v_1,\ldots,\ell_m \mapsto v_m\} \\ \theta(C') & = & \{\ell_1 \mapsto \tau_1,\ldots,\ell_m \mapsto \tau_m\} \end{array}$$

Typing Assumption:

1. $\mathtt{GU}(SS'\{\ell \mapsto v\})$
2. $\vdash SS'\{\ell \mapsto v\} : C$.
3. $\cdot;C;\cdot \vdash \mathtt{coerce}(\gamma);\iota$.

Where the coercion typing judgement is

$$\frac{\begin{array}{c}\Delta = \beta_1{:}\kappa_1,\ldots,\beta_n{:}\kappa_n \quad \cdot \vdash c_i : \kappa_i \quad (\text{for } 1 \le i \le n) \\ \cdot \vdash C = C'' \otimes \{\ell \mapsto \theta(\tau)\} \otimes \theta(C') : \mathtt{Store}\end{array}}{\begin{array}{c}\cdot;C \vdash \mathtt{pack}_{[c_1,\ldots,c_n \mid \theta(C')]\mathtt{as}\ \exists[\Delta \mid C'].\tau}(\ell) \implies \\ \cdot;C'' \otimes \{\ell \mapsto \exists[\Delta \mid C'].\tau\}\end{array}}$$

and the instruction typing judgement implies $\iota$ is well-formed:

$$\cdot;C'' \otimes \{\ell \mapsto \exists[\Delta \mid C'].\tau\};\cdot \vdash \iota$$

By inspection of the definition of $\mathtt{L}(\cdot)$, we can deduce that $\mathtt{L}(SS'\{\ell \mapsto v\}) = \mathtt{L}(S\{\ell \mapsto v'\})$. Therefore, since $\mathtt{GU}(SS'\{\ell \mapsto v\})$, we can conclude that (4) $\mathtt{GU}(S\{\ell \mapsto v'\})$.
From the definitions above, we know that

$$SS'\{\ell \mapsto v\} = S\{\ell_1 \mapsto v_1,\ldots,\ell_m \mapsto v_m, \ell \mapsto v\}$$

Moreover, the constraint equality judgement in the coercion typing judgement with the definition of $\theta(C')$ implies that

$$\cdot \vdash C = C'' \otimes \{\ell_1 \mapsto \tau_1,\ldots,\ell_m \mapsto \tau_m, \ell \mapsto \theta(\tau)\} : \mathtt{Store}$$

Now from (2) and by induction on $m$ and Lemma 14, we can conclude the following facts:

6. $\cdot;\cdot \vdash v : \theta(\tau)$
7. for $1 \le i \le m$, $\cdot;\cdot \vdash v_i : \tau_i$
8. $\vdash S : C''$

From (7), we can prove $\vdash S' : \theta(C')$ using the store typing rule. Consequently, we can show that $v'$ is well-formed:

$$\frac{\Delta = \beta_1{:}\kappa_1, \ldots, \beta_n{:}\kappa_n \qquad \cdot \vdash c_i : \kappa_i \quad (\text{for } 1 \le i \le n) \qquad \vdash S' : \theta(C') \qquad \cdot;\cdot \vdash v : \theta(\tau)}{\cdot;\cdot \vdash \mathtt{pack}_{[c_1,\ldots,c_n \mid S']\mathtt{as}\exists[\Delta \mid C'].\tau}(v) : \exists[\Delta \mid C'].\tau}$$

Since $\vdash S : C''$ and $\cdot;\cdot \vdash v' : \exists[\Delta \mid C'].\tau$, we can conclude by the store typing judgement that (8)

$$\vdash S\{\ell \mapsto v'\} : C'' \otimes \{\ell \mapsto \exists[\Delta \mid C'].\tau\}$$

Finally, using (4), (5), (8), we can conclude that $\vdash (S\{\ell \mapsto v'\}, \iota)$.

$\square$

**Lemma 19 (Progress)** *If $\vdash (S, \iota)$ then either $\iota = \mathtt{halt}\, i$ or $(S, \iota) \longmapsto_P (S', \iota')$.*

**Proof:** By cases on the syntax of the first instruction of $\iota$. The proof follows from Canonical Value Forms and Canonical Store Forms. Here, we show a couple of representative cases.

- $(S, \mathtt{new}\, \rho, x, i; \iota)$. This program always steps to

  $$(S\{\ell \mapsto \overbrace{\langle \mathcal{S}(0), \ldots, \mathcal{S}(0)\rangle}^{i}\}, \iota[\ell/\rho][\mathtt{ptr}(\ell)/x])$$

  where $\ell$ is some location not present in $S$.
- $(S, \mathtt{free}\, v; \iota)$.
  Typing Assumption:

  1. $\mathtt{GU}(S)$
  2. $\vdash S : C$.
  3. $\cdot; C; \cdot \vdash \mathtt{free}\, v; \iota$.

  The instruction typing judgement must have the form:

  $$\frac{\cdot;\cdot \vdash v : ptr(\ell) \qquad \cdot \vdash C = C' \otimes \{\ell \mapsto \langle \sigma_1, \ldots, \sigma_n\rangle\} : \mathtt{Store} \qquad \cdot; C'; \cdot \vdash \iota}{\cdot; C; \cdot \vdash \mathtt{free}\, v; \iota}$$

  By Canonical Value Forms, $v$ must be $\mathtt{ptr}(\ell)$. By Canonical Store Forms, $S = S'\{\ell \mapsto v'\}$ and $\cdot;\cdot \vdash v' : \langle \sigma_1, \ldots, \sigma_n\rangle$. By Canonical Value Forms again, $v'$ must be $\langle v_1, \ldots, v_n\rangle$. Therefore this program meets the precondition for the operational rule for `free` and it steps to $(S', \iota)$.
- $\mathtt{halt}\, v$. This program is not considered stuck if $v$ is an integer $i$. By inspection of the typing rule for halt, we see that

  $$\cdot;\cdot \vdash v : int$$

  By Canonical Value Forms, $v$ must be an integer $i$.
- $(S, \mathtt{coerce}(\gamma); \iota)$ where $\gamma = \mathtt{unpack}\, \ell\, \mathtt{with}\, \Delta$
  Typing Assumption:

  1. $\mathtt{GU}(S)$
  2. $\vdash S : C$.
  3. $\cdot; C; \cdot \vdash \mathtt{coerce}(\gamma); \iota$.

  Where the coercion typing judgement has the form:

  $$\frac{\cdot \vdash C = C'' \otimes \{\ell \mapsto \exists[\Delta \mid C'].\tau\} : \mathtt{Store}}{\cdot; C \vdash \mathtt{unpack}\, \ell\, \mathtt{with}\, \Delta \implies \Delta; C'' \otimes \{\ell \mapsto \tau\}@C'}$$

  and the instruction typing judgement implies $\iota$ is well-formed:

  $$\Delta; C'' \otimes \{\ell \mapsto \tau\}@C'; \cdot \vdash \iota$$

  By Canonical Store Forms, $S = S'\{\ell \mapsto v\}$ and

  $$\cdot;\cdot \vdash v : \exists[\Delta \mid C'].\tau$$

  By Canonical Value Forms,

  $$v = \mathtt{pack}_{[c_1,\ldots,c_n \mid S'']\mathtt{as}\exists[\Delta \mid C'].\tau}(v')$$

  By inspection of the definition of $\mathtt{GU}(S)$, we can conclude that $(Dom(S') \cup \{\ell\}) \cap Dom(S'') = \emptyset$. Therefore, $S'S''\{\ell \mapsto v\}$ is a store. Canonical Value Forms also implies that $\Delta = \beta_1{:}\kappa_1, \ldots, \beta_n{:}\kappa_1$ and therefore $[c_1, \ldots, c_n/\Delta]$ is a substitution. Therefore,

  $$(S, \mathtt{coerce}(\gamma); \iota) \longmapsto_P (S'S''\{\ell \mapsto v'\}, \iota[c_1, \ldots, c_n/\Delta])$$

**Definition 20 (Stuck Program)** *A program $(S, \iota)$ is stuck if no operational rule applies and $\iota$ is not $\mathtt{halt}\, i$.*

**Theorem 21 (Type Soundness)** *If $\vdash (S, \iota)$ and $(S, \iota) \longmapsto_P^* (S', \iota')$ then $(S', \iota')$ is not stuck.*

**Proof:** By induction on the length of the evaluation sequence. Uses Progress and Preservation.