Quasi-Linear Types*

Naoki Kobayashi
Department of Information Science, University of Tokyo
7-3-1 Hongo,Bunkyo-ku, Tokyo 113-0033, Japan
email:koba@is.s.u-tokyo.ac.jp

November 13, 1998

Abstract

Linear types (types of values that can be used just once) have been drawing a great deal of attention because they are useful for memory management, in-place update of data structures, etc.: an obvious advantage is that a value of a linear type can be immediately deallocated after being used. However, the linear types have not been applied so widely in practice, probably because linear values (values of linear types) in the traditional sense do not so often appear in actual programs. In order to increase the applicability of linear types, we relax the condition of linearity by extending the types with information on an evaluation order and simple dataflow information. The extended type system, called a quasi-linear type system, is formalized and its correctness is proved. We have implemented a prototype type inference system for the core-ML that can automatically find out which value is linear in the relaxed sense. Promising results were obtained from preliminary experiments with the prototype system.

1 Introduction

1.1 Linear types

A number of type systems based on Girard's linear logic [6] have been proposed for functional languages [1, 3, 13, 21] and concurrent languages [9, 12]. They guarantee that certain data structures (called *linear* values) are accessed just once (or at most once). The distinction between linear values

*This is a revised version of the technical report TR98-02 from Department of Information Science, University of Tokyo. A summary will be presented at ACM POPL'99.

and other values provides many benefits: improvement of memory management [1], safe inlining [21], etc. Among them, we are here interested in the improvement of memory management. If some data structure is statically known to be linear, it can be deallocated immediately after it is accessed. Moreover, if another heap value needs to be created after a linear value is accessed, we can just replace the linear value with the new value, instead of deallocating the linear value and allocating space for the new data (provided that the physical size of the new value is not greater than that of the linear value). For instance (throughout this paper, we assume a call-by-value language), when the function $\lambda\langle x, y\rangle.\langle x, y+1\rangle$ is called, if the argument is a linear pair, the second element y of the pair can be destructively updated to $y+1$. Similarly, the "append" of linear lists can be performed destructively, without copying cons cells. This kind of improvement will be especially effective for functional programs, because many intermediate data structures like cons cells and closures are created in naive functional programs.

1.2 Limitation of linear types

In spite of the above-mentioned benefit from linear type systems, they do not seem to have been used so widely, even after type inference algorithms [8, 9, 21] were proposed that can automatically find which values are linear.

We think one of the major reasons for this is that linear type systems are too naive for the above application: what is actually important for automatic deallocation and in-place update is to identify which is the last access to a heap value; the condition of linearity is too strong for this purpose. For example, consider an expression $M \equiv \textbf{let}\ x = 2.0\ \textbf{in let}\ y = x + 1.0\ \textbf{in}\ y + x$: it is easy to see that $y + x$ is the last access to x, but linear type systems cannot insert a code to deallocate x — just because x is used twice! This limitation also forces a programmer to follow a particular programming style. For instance, in $\lambda z.\langle \textbf{fst}(z), \textbf{snd}(z) + 1\rangle$, the pair z is judged to be accessed twice; so, if one wants the pair to be deallocated, one must write $\lambda\langle x, y\rangle.\langle x, y+1\rangle$ instead.

1.3 Our proposal — almost linear types (quasi-linear types)

In order to remove the above-mentioned limitation of linear types, we relax the condition of linearity.

A key idea is to express information on the evaluation order and dataflow by using types. Recall the above expression M: if a type system can take it into account that $x + 1.0$ is evaluated before $y + x$, it can ignore the use of x in $x + 1.0$ and treat the above expression in the same way as $\textbf{let}\ x = 2.0\ \textbf{in let}\ y = 1.0\ \textbf{in}\ y + x$. In order to obtain such information on the evaluation order, the type system should also be able to deal with some dataflow information. Consider, for example, an expression $\textbf{let}\ y = f(x)\ \textbf{in}\ g(x) + h(y)$. $f(x)$ is evaluated before $g(x)$ but it does not imply that the access to x in $g(x)$ is the last one: x may be returned by $f(x)$ and accessed again in $h(y)$. In order

to deal with this, we distinguish between the type of a value that must be used up in an expression and the type of a value that may be returned as a part of the evaluation result of an expression.

It would be possible to obtain the above kinds of information by using more sophisticated analyses, but we instead obtain it by a very simple method — by introducing a new *use* [9, 21]. Advantages of that approach include: (1) the whole analysis can be formalized uniformly in terms of a type system (this is especially advantageous when we introduce polymorphism) and (2) a program containing free variables can be analyzed as long as their type information is provided, which is useful for modular (or incremental) analysis and separate compilation of programs. We first review the ideas of previous linear type systems [9, 21] and then overview the ideas of our system below.

1.3.1 Review of linear type systems

A *use* was introduced to control how often values can be accessed [9, 21]: it was either 0 (not used at all), 1 (accessed at most once), or ω (accessed an arbitrary number of times) in [9] and was either 1 or ω in [21]. Types are annotated with such uses. For example, real^1 represents the type of real numbers that can be accessed at most once, and $\mathit{int} \to^{\omega} \mathit{int}$ is the type of functions on integers that can be called an arbitrary number of times. A type judgment can be accordingly refined so that it gives more useful information than the ordinary one: for example, $x : \mathit{real}^1 \vdash N : \mathit{real}^{\omega}$ means not only that x is used as a real number in N but also that it is used at most once. So, it is invalid if N is $\mathbf{let}\ y = x + 1.0\ \mathbf{in}\ x + y$.

The following type derivation highlights a key point of the linear type system:

$$\frac{x : \mathit{real}^1 \vdash x + 1.0 : \mathit{real}^1 \qquad x : \mathit{real}^1, y : \mathit{real}^1 \vdash x + y : \mathit{real}^1}{x : \mathit{real}^1 + x : \mathit{real}^1 (= x : \mathit{real}^{\omega}) \vdash \mathbf{let}\ y = x + 1.0\ \mathbf{in}\ x + y : \mathit{real}^1}$$

The premises of the derivation imply that x is used once each in $x + 1.0$ and $x + y$. In order to know how x is totally used in the expression, we combine the type environments of subexpressions by *adding* the corresponding uses as above. This is in contrast to the following rule of ordinary type systems, where type environments are *shared* between subexpressions:

$$\frac{\Gamma \vdash M_1 : \tau_1 \qquad \Gamma, y : \tau_1 \vdash M_2 : \tau_2}{\Gamma \vdash \mathbf{let}\ y = M_1\ \mathbf{in}\ M_2 : \tau_2}$$

By using the linear type system, we can infer how often each heap value is accessed, and annotate each allocation with a use. For instance, we can annotate the expression M as $\mathbf{let}\ x^{\omega} = 2.0\ \mathbf{in}\ \mathbf{let}\ y^1 = x + 1.0\ \mathbf{in}\ x + y$, so that y is deallocated after it is accessed in $x + y$ while x is not deallocated.

1.3.2 Overview of our type system

In order to express simple dataflow information, we introduce another use δ. Intuitively, a value with use δ (which we call a *δ-value* below) may be accessed many times but only *locally* — it cannot be returned as (a part of) the computed result.[1] So, x can have type real^{δ} in $x+1.0$ and $(\lambda y.(y+1.0))x$, but not in $\langle x, 1.0\rangle$ or $\lambda y.x+y$. A value with use 1 (hereafter, we call it a *quasi-linear* value or simply a *linear* value, and call a use-once value in the traditional sense a *strictly linear* value) can now be accessed in a more relaxed manner: It can be accessed many times as a δ-value, and then it can be accessed as a strictly linear value (i.e., as a value that can be accessed once and deallocated).

In order to guarantee such usage of a value, it is crucial that the type system can take the evaluation order into account. The type derivation shown above is now changed as follows:

$$\frac{x : \mathit{real}^{\delta} \vdash x + 1.0 : \mathit{real}^{1} \qquad x : \mathit{real}^{1}, y : \mathit{real}^{1} \vdash x + y : \mathit{real}^{1}}{x : \mathit{real}^{\delta}; x : \mathit{real}^{1} (= x : \mathit{real}^{1}) \vdash \mathbf{let}\ y = x + 1.0\ \mathbf{in}\ x + y : \mathit{real}^{1}}$$

Here, the new combination $(x : \mathit{real}^{\delta}); (x : \mathit{real}^{1})$ of type environments captures the fact that x is first accessed as a δ-value in $x + 1.0$, and then it is accessed as a linear value in $x + y$. Thus, x can be deallocated after $x + y$ is evaluated. Similarly, even if one writes $\lambda z.\langle \mathbf{fst}(z), \mathbf{snd}(z) + 1\rangle$ instead of $\lambda\langle x, y\rangle.\langle x, y + 1\rangle$, z can be deallocated after $\mathbf{snd}(z)$ is evaluated.

Because a quasi-linear value may be used more than once, in addition to allocation of a heap value, each access to a heap value is also annotated with a use: it is for distinguishing between the last access of the value and the other accesses. For example, the expression M is annotated as $\mathbf{let}\ x^{1} = 2.0\ \mathbf{in}\ \mathbf{let}\ y^{1} = x^{\delta} + 1.0\ \mathbf{in}\ y^{1} + x^{1}$ (actually, we will annotate constructors and destructors of heap values instead of variables). Here, we annotate x in $y + x$ with 1 in order to indicate that it is the last access, while x in $x + 1.0$ is annotated with δ in order to indicate that it is not the last one.

1.4 Main results

Main contributions of the present work are formalization of the new type system sketched above and a proof of its correctness. Since the evaluation order must be taken into account, the proof is non-trivial and more involved than that of previous type systems.

Another contribution is implementation of a type inference system for the core-ML (i.e., Standard ML without modules [14]) based on the new type system, which inputs an unannotated core-ML expression and outputs a use-annotated expression. We have so far tested several fairly small programs and obtained promising results: for programs that use lists frequently (such as sorting programs, the

[1] Intuition behind the name δ is that it is something between 0 and 1, and that it can be almost ignored compared with 1.

sieve of Eratosthenes and Conway's game of life), the type inference system could judge that most heap values (in the case of the sorting programs and the sieve of Eratosthenes, all values except for top-level functions) are linear, which indicates that they can be executed almost without garbage collection. Moreover, the annotated programs output by the system indicate that most linear cons cells in those programs can be updated in-place (the application of linear types to the in-place quick sort has been suggested by Baker [2] but a remarkable point here is that it can be performed for naive programs with no programmer's annotation).

1.5 Structure of the paper

The rest of this paper is structured as follows. Section 2 introduces the syntax of the target language. Section 3 gives our type system for judging whether an expression is correctly annotated with uses. Section 4 shows the correctness of the type system and Section 5 briefly explains how to obtain a type inference algorithm that can automatically infer use annotation. Section 6 discusses several extensions of the target language. Section 7 explains our prototype type inference system and the results of preliminary experiments. Section 8 discusses related work and Section 9 concludes this paper.

2 Syntax and Operational Semantics of the Target Language

In this section, we introduce the syntax and operational semantics of (use-annotated) expressions.

2.1 Uses

As explained in Section 1, a *use* is introduced to control how often and in which way each heap value can be accessed.

Definition 2.1 [uses]: A use is 0, δ, 1, or ω.

We use metavariables $\kappa_1, \kappa_2, \ldots$ for uses.

As mentioned in Section 1, a new point here is the use δ: basically, we say that a heap value is accessed in an expression as a value of use δ if it is accessed *locally* inside the expression and cannot be returned as a part of the evaluation result. 0 means that the data cannot be accessed at all, 1 means that after the data is accessed in a restricted manner as a value of use δ, it can be either (1) accessed at most once and deallocated inside the current expression being evaluated or (2) put into the evaluation result as a value of use 1. ω means that the data can be accessed many times in any way.

A value of use ω can be regarded as a value of any other use, and a value of 1 can be regarded as a value of use δ or 0. In order to express this kind of relationship between uses, we define a total order $\leq$ on uses by $0 \leq \delta \leq 1 \leq \omega$. We write $\kappa_1 < \kappa_2$ if $\kappa_1 \neq \kappa_2$ and $\kappa_1 \leq \kappa_2$.

Remark 2.2: By a heap value being *accessed* (or *used*), we mean the contents of the heap value are indeed read; so, just passing the reference to the heap value does not count as access. For example, we do not say that y is accessed in $(\lambda x.x)y$, since the expression can be reduced to y without reading the actual contents of y. A pair is considered to be accessed only when its first or second element is extracted, a closure is accessed only when it is invoked, and a real number is accessed only when it is passed as an argument to a primitive function on real numbers.

2.2 Expressions

We consider a simply-typed λ-calculus with recursion and pairs as a target language. Its extension with polymorphism and other data structures will be briefly discussed in Section 6. Because our type system is sensitive to an evaluation order, we use the K-normal form [5] in order to make the evaluation order explicit and name each intermediate value. (For readability, we sometimes use expressions that are not in K-normal form when giving examples.)

The syntax of expressions is given below. Each allocation or read operation of a heap value is annotated with a use. The annotation can be automatically inferred by a type inference algorithm explained in Section 5.

Definition 2.3 [expressions]:

$$
\begin{array}{rcl}
M & ::= & V \mid \textbf{let } x = \langle V_1, V_2 \rangle^{\kappa} \textbf{ in } M \mid \textbf{let } x = \textbf{fst}^{\kappa}(y) \textbf{ in } M \mid \textbf{let } x = \textbf{snd}^{\kappa}(y) \textbf{ in } M \\
 & & \mid \textbf{let } x = \lambda^{\kappa} y.M_1 \textbf{ in } M_2 \mid \textbf{let } x = \textbf{rec}^{\kappa}(f, y, M_1) \textbf{ in } M_2 \mid \textbf{let } x = \mathit{apply}^{\kappa}(y, V) \textbf{ in } M \\
 & & \mid \textbf{let } x = M_1 \textbf{ in } M_2 \mid \textbf{if0 } V \textbf{ then } M_1 \textbf{ else } M_2 \\
V & ::= & x \mid n
\end{array}
$$

We write $\mathcal{E}$ for the set of expressions.

The metavariable V represents a value that can be represented in one word and need not be allocated in the heap. Here, it is either an integer constant (denoted by n) or a variable (denoted by x). A variable can be considered a heap address.

$\langle V_1, V_2 \rangle^{\kappa}$ and $\lambda^{\kappa} y.M_1$ allocate a pair and a closure respectively in the heap, and records that their use is κ (which shall be restricted to $0, 1$, or ω by the type system given later). The recorded use expresses how the value can be accessed in the rest of the computation: 0 means that the value cannot be accessed at all (so, $\langle V_1, V_2 \rangle^0$ actually need not allocate the pair in the heap), 1 means that the value can be accessed as a linear value and may be deallocated later, and ω means that the value can be accessed in an arbitrary manner and can be deallocated only by other mechanisms such as garbage collection. $\textbf{rec}^{\kappa}(f, y, M_1)$ creates a recursive function f such that $f(y) = M_1$.

There are three operations to access the heap: $\mathbf{fst}^\kappa(x)$ ($\mathbf{snd}^\kappa(x)$, resp.) extracts the first (second, resp.) element of the pair stored at x, and $apply^\kappa(y, V)$ reads the closure stored at y and applies it to V. κ attached to an access operation represents as a value of what use the heap value is accessed by this operation. If κ is δ, the heap is just read and unchanged; if it is 1, the heap value is deallocated after being read (if the use of the heap value is also 1[2]). If κ is ω, then the operation assumes that the accessed heap value is an ω-value and does not deallocate the value (so, ω is the same as δ in effect and is unnecessary; it is included just for technical convenience). If κ is greater than the actual use recorded at the accessed address, the access is invalid and causes an error.

A conditional expression **if0** V **then** M_1 **else** M_2 is reduced to M_1 if $V = 0$ and otherwise reduced to M_2.

Example 2.4: **let** $x = \langle 1, 2\rangle^1$ **in let** $y = \mathbf{fst}^\delta(x)$ **in** **let** $z = \mathbf{snd}^1(x)$ **in** z allocates a linear pair $\langle 1, 2\rangle$ in the heap, and then reads its first element; at this moment, x is not deallocated since **fst** is annotated with δ. After that, the second element is read and the pair is deallocated.

2.3 Operational semantics

In order to clarify how use annotation is used for allocating/deallocating heap values at run-time, we define an operational semantics as a rewriting relation on pairs of a heap and an expression [16, 21].

Definition 2.5 [evaluation contexts]: The set of *evaluation contexts* is given by the following syntax:

$$C[\,] ::= [\,] \mid \mathbf{let}\ x = C[\,]\ \mathbf{in}\ M.$$

We write $C[M]$ for the expression obtained from $C[\,]$ by replacing the hole $[\,]$ with M.

Definition 2.6 [heap]: A *heap value*, denoted by h, is a term of the form $\langle V_1, V_2\rangle$ or $\lambda x.M$. A *heap* is a mapping from a finite set of variables to pairs consisting of a use and a heap value. We write $\{x_1 \mapsto^{\kappa_1} h_1, \ldots, x_n \mapsto^{\kappa_n} h_n\}$ for a heap H such that $H(x_i) = (\kappa_i, h_i)$.

The use associated with a heap value is used for judging whether the value can be deallocated after it is accessed as a linear value: the value can be deallocated only if the use is 1. The use 0 means that the value has been already deallocated. We often write h^κ for $\langle V_1, V_2\rangle^\kappa$ or $\lambda^\kappa x.M$. We write $\mathcal{H}$ for the set of heaps.

The reduction relation $\rightsquigarrow \in (\mathcal{H} \times \mathcal{E}) \times ((\mathcal{H} \times \mathcal{E}) \cup \{\mathbf{Error}\})$ is defined by the rules given in Figure 1. **Error** indicates that invalid access to the heap has occurred (there are other kinds of errors such

[2]The check of the use of the heap value is necessary, because we allow an ω-value to be accessed as a linear value. If we forbid such coercion of an ω-value into a linear value as in [21], then the check is unnecessary. However, we prefer not to make such restriction because the check can be implemented efficiently (see Remark 2.7).

as application of a non-function to a value, etc.; however, because the lack of those errors can be guaranteed by a type system in the usual way, this paper focuses on errors caused by invalid heap access).

The first two rules (R-Heap) and (R-Rec) are for allocating heap values. The use κ is recorded at a new address together with the allocated value. The heap is not changed in (R-SVal) since V is a one-word value.

The rules (R-App) and (R-App-Error) for function application deserve attention. Since $\mathit{apply}^{\kappa'}(x, V)$ reads a closure stored at x as a value with use κ', the currently available use κ of x should be greater than or equal to κ': otherwise, the application causes an error. If $\kappa = \kappa' = 1$, the closure is deallocated after the application and it can no longer be called; so, the use of x should be changed to 0. It is expressed by the subtraction $\kappa - \kappa'$, whose definition is given in Figure 2. Similarly, access to a pair $\mathbf{fst}^{\kappa'}(x)$ or $\mathbf{snd}^{\kappa'}(x)$ succeeds only if $\kappa \geq \kappa'$, and the use is decreased by κ' after the access ((T-Fst) — (T-Snd-Error)).

Remark 2.7: One may think that the above operation on uses incurs a heavy overhead at run-time. However, because the type system guarantees that no invalid access occurs, the check of $\kappa \geq \kappa'$ is always guaranteed to succeed and can be eliminated. Moreover, the use associated with a heap value can change only from 1 to 0; since this change means that the heap value is deallocated in the actual implementation, the use need not be updated actually. This further implies that the use of a heap value can be recorded not in the heap space itself but in the pointer to it by using a one-bit tag, and that the extra run-time cost is only to check this tag (to know whether the use of the accessed heap value is 1 or ω) when the access operation is annotated with 1. So, we think the actual run-time overhead is quite small.

Example 2.8: The expression in Example 2.4 is reduced as follows:

$$
\begin{array}{ll}
 & (\{\}, \mathbf{let}\ x = \langle 1,2\rangle^1\ \mathbf{in\ let}\ y = \mathbf{fst}^{\delta}(x)\ \mathbf{in\ let}\ z = \mathbf{snd}^{1}(x)\ \mathbf{in}\ z) \\
\leadsto & (\{u \mapsto^1 \langle 1,2\rangle\}, \mathbf{let}\ y = \mathbf{fst}^{\delta}(u)\ \mathbf{in\ let}\ z = \mathbf{snd}^{1}(u)\ \mathbf{in}\ z) \\
\leadsto & (\{u \mapsto^1 \langle 1,2\rangle\}, \mathbf{let}\ y = 1\ \mathbf{in\ let}\ z = \mathbf{snd}^{1}(u)\ \mathbf{in}\ z) \\
\leadsto & (\{u \mapsto^1 \langle 1,2\rangle\}, \mathbf{let}\ z = \mathbf{snd}^{1}(u)\ \mathbf{in}\ z) \\
\leadsto & (\{u \mapsto^0 \langle 1,2\rangle\}, \mathbf{let}\ z = 2\ \mathbf{in}\ z) \\
\leadsto & (\{u \mapsto^0 \langle 1,2\rangle\}, 2)
\end{array}
$$

The heap value u is considered to be deallocated when the use changes from 1 to 0.

Example 2.9: If the expression in Example 2.4 is wrongly annotated as:

$$\mathbf{let}\ x = \langle 1,2\rangle^1\ \mathbf{in\ let}\ y = \mathbf{fst}^{1}(x)\ \mathbf{in\ let}\ z = \mathbf{snd}^{\delta}(x)\ \mathbf{in}\ z,$$

$$(H, C[\textbf{let } x = h^{\kappa} \textbf{ in } M]) \rightsquigarrow (H\{y \mapsto^{\kappa} h\}, C[[y/x]M]) \ (y \text{ fresh}) \quad \text{(R-Heap)}$$

$$(H, C[\textbf{let } x = \textbf{rec}^{\kappa}(f, y, M_1) \textbf{ in } M]) \rightsquigarrow (H\{z \mapsto^{\kappa} \lambda y.[z/f]M_1\}, C[[z/x]M]) \ (z \text{ fresh}) \quad \text{(R-Rec)}$$

$$(H, C[\textbf{let } x = V \textbf{ in } M]) \rightsquigarrow (H, C[[V/x]M]) \quad \text{(R-SVal)}$$

$$\frac{\kappa \geq \kappa' > 0}{(H\{x \mapsto^{\kappa} \lambda y.M\}, C[apply^{\kappa'}(x, V)]) \rightsquigarrow (H\{x \mapsto^{\kappa-\kappa'} \lambda y.M\}, C[[V/y]M])} \quad \text{(R-App)}$$

$$\frac{(\kappa < \kappa') \vee (\kappa' = 0)}{(H\{x \mapsto^{\kappa} \lambda y.M\}, C[apply^{\kappa'}(x, V)]) \rightsquigarrow \textbf{Error}} \quad \text{(R-App-ERROR)}$$

$$\frac{\kappa \geq \kappa' > 0}{(H\{x \mapsto^{\kappa} \langle V_1, V_2\rangle\}, C[\textbf{fst}^{\kappa'}(x)]) \rightsquigarrow (H\{x \mapsto^{\kappa-\kappa'} \langle V_1, V_2\rangle\}, C[V_1])} \quad \text{(R-Fst)}$$

$$\frac{(\kappa < \kappa') \vee (\kappa' = 0)}{(H\{x \mapsto^{\kappa} \langle V_1, V_2\rangle\}, C[\textbf{fst}^{\kappa'}(x)]) \rightsquigarrow \textbf{Error}} \quad \text{(R-Fst-Error)}$$

$$\frac{\kappa \geq \kappa' > 0}{(H\{x \mapsto^{\kappa} \langle V_1, V_2\rangle\}, C[\textbf{snd}^{\kappa'}(x)]) \rightsquigarrow (H\{x \mapsto^{\kappa-\kappa'} \langle V_1, V_2\rangle\}, C[V_2])} \quad \text{(R-Snd)}$$

$$\frac{(\kappa < \kappa') \vee (\kappa' = 0)}{(H\{x \mapsto^{\kappa} \langle V_1, V_2\rangle\}, C[\textbf{snd}^{\kappa'}(x)]) \rightsquigarrow \textbf{Error}} \quad \text{(R-Snd-Error)}$$

$$(H, C[\textbf{if0 } 0 \textbf{ then } M_1 \textbf{ else } M_2]) \rightsquigarrow (H, C[M_1]) \quad \text{(R-IfT)}$$

$$\frac{n \neq 0}{(H, C[\textbf{if0 } n \textbf{ then } M_1 \textbf{ else } M_2]) \rightsquigarrow (H, C[M_2])} \quad \text{(R-IfF)}$$

Figure 1: Operational Semantics

$\kappa_1 \backslash \kappa_2$	0	δ	1	ω
0	0	undef	undef	undef
δ	δ	δ	undef	undef
1	1	1	0	undef
ω	ω	ω	ω	ω

Figure 2: Definition of $\kappa_1 - \kappa_2$

then it is reduced to **Error** as follows:

$$
\begin{array}{ll}
 & (\{\}, \mathbf{let}\ x = \langle 1,2\rangle^1\ \mathbf{in\ let}\ y = \mathbf{fst}^1(x)\ \mathbf{in\ let}\ z = \mathbf{snd}^\delta(x)\ \mathbf{in}\ z) \\
\leadsto & (\{u \mapsto^1 \langle 1,2\rangle\}, \mathbf{let}\ y = \mathbf{fst}^1(u)\ \mathbf{in\ let}\ z = \mathbf{snd}^\delta(u)\ \mathbf{in}\ z) \\
\leadsto & (\{u \mapsto^0 \langle 1,2\rangle\}, \mathbf{let}\ y = 1\ \mathbf{in\ let}\ z = \mathbf{snd}^\delta(u)\ \mathbf{in}\ z) \\
\leadsto & (\{u \mapsto^0 \langle 1,2\rangle\}, \mathbf{let}\ z = \mathbf{snd}^\delta(u)\ \mathbf{in}\ z) \\
\leadsto & \mathbf{Error}
\end{array}
$$

3 Type System

As was shown in Example 2.9, if an expression is wrongly annotated with uses, a run-time error may occur. In order to reject such expressions, we introduce a type system. Our type system is a conservative extension of the usual type system for the simply typed λ-calculus in the sense that any expressions well-typed in the usual type system are well typed also in our type system.

There are two major differences between our quasi-linear type system and the usual linear type systems. As explained in Section 1, a linear value can be accessed many times as long as the last access is identified by the quasi-linear type system. The other difference is the interpretation of a pair type (see below).

3.1 Types

Types are used for expressing how often and in which way values can be used. Each instance of type constructor for product and arrow types is annotated with uses.

Definition 3.1 [types]: The set of types, ranged over by τ, is given by the following syntax.

$$\tau \quad ::= \quad int \mid \tau_1 \times^\kappa \tau_2 \mid \tau_1 \rightarrow^{\kappa_1,\kappa_2} \tau_2$$

κ of $\tau_1 \times^\kappa \tau_2$ and κ_1 of $\tau_1 \rightarrow^{\kappa_1,\kappa_2} \tau_2$ expresses how often and in which way a pair and a closure can be accessed. We require κ_2 of $\tau_1 \rightarrow^{\kappa_1,\kappa_2} \tau_2$ not to be δ. It represents how often (0, 1, or ω) the closure can be invoked in the sense of previous linear type systems [9, 21]. The closure itself is allocated and deallocated based on κ_1. The reason why we keep κ_2 will become clear when we present a typing rule for closure creations.

Note that the meaning of a pair type is different from that in previous linear type systems [8, 21]. In the previous linear type systems, $int \times^\omega (int \times^1 int)$ corresponds to the linear logic formula $!(int \otimes (int \otimes int))$; so, if a pair $\langle 1, \langle 2,3\rangle\rangle$ has this type, it can be read an arbitrary number of times, and *each time* the second element $\langle 2,3\rangle$ is extracted, it can be read at most once. On the other hand, in our quasi-linear type system, the second element $\langle 2,3\rangle$ can be accessed only linearly *throughout all the access* to the pair $\langle 1, \langle 2,3\rangle\rangle$ (not each time $\langle 2,3\rangle$ is extracted).

Example 3.2: $(int \times^{\delta} int) \rightarrow^{1,\omega} int$ is the type of a linear closure that takes a pair of integers as an argument, uses it locally, and returns an integer. The function may be invoked many times (thus its use is ω in the strict sense), but it can be invoked only linearly in the relaxed sense (i.e., invoked as a closure of use δ except for the last invocation). For example, $\lambda^1 x.(\mathbf{fst}^{\delta}(x) + \mathbf{snd}^{\delta}(x))$ can have this type.

Example 3.3: Consider an expression
let $f = \lambda^{\omega} z.(\mathbf{fst}^{\delta}(x) + z)$ **in let** $y = \mathbf{fst}^1(\mathbf{snd}^{\delta}(x))$ **in** M and suppose x does not appear in M. Because the second element of the pair x is accessed just once in $\mathbf{fst}^1(\mathbf{snd}^{\delta}(x))$, it can be assigned the type $int \times^{\omega} (int \times^1 int)$; so, the pair of integers can be deallocated at $\mathbf{fst}^1$. Consider another expression **let** $f = \lambda^1 z.(\mathbf{fst}^1(\mathbf{snd}^1(z)) + 1)$ **in** $apply^{\delta}(f, x) + apply^1(f, x)$. The second element of x is accessed once (by $\mathbf{fst}^1$) each time it is extracted by $\mathbf{snd}^1(z)$. Since it is totally accessed more than once, the type $int \times^{\omega} (int \times^{\omega} int)$ is assigned to x in our quasi-linear type system.

3.2 Type judgment

A type judgment is of the form $\Gamma \vdash M : \tau$, where Γ (called a type environment) is a mapping from a finite set of variables to types. It expresses how each heap value is accessed during evaluation of M. For example, $x : int \times^{\delta} int \vdash M : int \times^1 int$ implies $(1)M$ may access the heap address x, $(2)$the result is a linear pair of integers, and $(3)x$ is used up in M and does not escape through the result.

Notation 3.4: We write $V_1 : \tau_1, \ldots, V_n : \tau_n$ for the type environment Γ such that $dom(\Gamma) = \{V_1, \ldots, V_n\} \cap \mathcal{V}$ and $\Gamma(V_i) = \tau_i$ for each $V_i \in dom(\Gamma)$, where $\mathcal{V}$ denotes the set of variables. For example, $(x : int, 2 : int)$ denotes the type environment that maps x to int. If $V \notin dom(\Gamma)$, we write $\Gamma, V : \tau$ for the type environment Γ' such that (1) $\Gamma' = dom(\Gamma) \cup (\{V\} \cap \mathcal{V})$ and (2) $\Gamma'(x) = \tau$ if $x \in (\{V\} \cap \mathcal{V})$ and $\Gamma'(x) = \Gamma(x)$ if $x \in dom(\Gamma)$.

3.3 Operations on uses, types, and type environments

In presenting typing rules, we use several operations on uses, types, and type environments given in Figure 3 and 4. As explained in Section 1, the operation $\kappa_1 + \kappa_2$ is used for computing the total use of a value when it is accessed as κ_1 in one place and as κ_2 in another place. When the order of the uses is statically known, $\kappa_1; \kappa_2$ is used instead. $\lceil \kappa \rceil$ is the least non-δ use that is greater than or equal to κ, and $\lfloor \kappa \rfloor$ is the greatest non-δ use that is less than or equal to κ. $\kappa_1 \cdot \kappa_2$ is used for computing the total use of a value when the value is accessed κ_1 times as a κ_2-value. Motivations for these operations will become clearer when typing rules are given below.

These operations are extended to operations on types and type environments. For example, if a heap value is accessed as a value of type $int \times^{\delta} int$ in one place and as a value of type $int \times^1 int$ in

another place, it is totally accessed as a value of type $(int \times^{\delta} int) + (int \times^{1} int) = int \times^{\omega} int$, which means that the value may be accessed more than once.

The definitions of operations on pair types and function types deserve special attention; notice that the operations act on sub-components of pair type, but not on the arguments and return types of functions. In order to understand the reason for this, suppose x is accessed in two places, each as a value of type $(int \times^{1} int) \times^{1} int$ (i.e., the inner pair of integers and the outer pair are both accessed linearly). Then, both the inner pair of integers and the outer pair are totally accessed more than once; it is expressed by the type $(int \times^{1+1} int) \times^{1+1} int$ obtained by adding each use attached to the pair types, not by the type $(int \times^{1} int) \times^{1+1} int$ (which means that the inner pair is totally accessed only linearly). On the other hand, suppose x is accessed in two places as a function of type $(int \times^{1} int) \rightarrow^{1,1} (int \times^{1} int)$. Then, the function is invoked twice, and each time it is invoked, it uses an argument pair linearly and returns a linear pair. So, the total access to the function is expressed by $(int \times^{1} int) \rightarrow^{1+1,1+1} (int \times^{1} int)$, not by $(int \times^{1+1} int) \rightarrow^{1+1,1+1} (int \times^{1+1} int)$. Similarly, the operation $\lceil \cdot \rceil$ also acts on sub-components of pair type but not on the arguments and return types of function types. This is because $\lceil \tau \rceil$ is intended to express the type of an expression whose evaluation result does not contain δ-values. Although the type $(int \times^{\delta} int) \rightarrow^{1,1} (int \times^{1} int)$ contains δ, it just means that a function of that type uses an argument pair locally, not that the function must be used locally. So, $\lceil (int \times^{\delta} int) \rightarrow^{1,1} (int \times^{1} int) \rceil = (int \times^{\delta} int) \rightarrow^{1,1} (int \times^{1} int)$.

We often omit $\cdot$ and write $\kappa_1 \kappa_2$ for $\kappa_1 \cdot \kappa_2$ and $\kappa\Gamma$ for $\kappa \cdot \Gamma$. We give higher precedence to $\cdot$, $+$, and ; in this order.

Example 3.5: Let τ_1 be $int \times^{\delta} (int \times^{\delta} int)$ and τ_2 be $int \times^{1} (int \times^{0} int)$. Then,

$$\begin{array}{lcl} \tau_1 + \tau_2 & = & int \times^{\omega} (int \times^{\delta} int) \\ \tau_1 ; \tau_2 & = & int \times^{1} (int \times^{\delta} int) \\ \lceil \tau_1 \rceil & = & int \times^{1} (int \times^{1} int) \\ \omega \cdot \tau_1 & = & int \times^{\omega} (int \times^{\omega} int). \end{array}$$

$$\begin{array}{lcl} (x : \tau_1, y : \tau_1) + (x : \tau_2) & = & x : (\tau_1 + \tau_2), y : \tau_1 \\ & = & x : int \times^{\omega} (int \times^{\delta} int), y : int \times^{\delta} (int \times^{\delta} int). \end{array}$$

3.4 Typing rules

3.4.1 Variables, constants, and weakening

The rule for variables and constants is:

$$V : \tau \vdash V : \tau \qquad \text{(T-VAL)}$$

If an expression is well typed under some type environment, then it should also be well typed under a type environment that represents more access capabilities. For example, if $x : \mathit{int} \times^1 \mathit{int} \vdash M : \mathit{int}$, then $x : \mathit{int} \times^\omega \mathit{int} \vdash M : \mathit{int}$, since the former judgment requires x to be used as a linear pair, while the latter does not impose such a requirement. The following rule allows such weakening of an assumption:

$$\frac{\Gamma' \vdash M : \tau \qquad \Gamma' \leq \Gamma}{\Gamma \vdash M : \tau} \qquad \text{(T-Weak)}$$

The relation $\Gamma' \leq \Gamma$, which means "Γ represents more access capabilities than Γ' (in other words, Γ allows more liberal access to the heap)," is defined in Figure 4.

3.4.2 Allocation of heap values

Let us consider an expression $\mathbf{let}\ x = \langle y, z \rangle^\kappa\ \mathbf{in}\ M$. In M, y and z can be accessed in two ways: either directly by using addresses y and z, or through the pair x (by extracting y and z). If $\Gamma, x : \tau_1 \times^\kappa \tau_2 \vdash M : \tau$, then the access in the former way is represented by the types $\Gamma(y)$ and $\Gamma(z)$, while the access in the latter way is represented by the types τ_1 and τ_2. Therefore, information on the total access is obtained by adding those types. For example, if $\Gamma(y) = \mathit{int} \times^1 \mathit{int}$ and $\tau_1 = \mathit{int} \times^1 \mathit{int}$, then the total access to y can be represented by $\Gamma(y) + \tau_1 = \mathit{int} \times^\omega \mathit{int}$. Thus, the rule for the allocation of a pair is:

$$\frac{\Gamma, x : \tau_1 \times^\kappa \tau_2 \vdash M : \tau_3 \qquad \kappa \neq \delta}{\Gamma + V_1 : \tau_1 + V_2 : \tau_2 \vdash \mathbf{let}\ x = \langle V_1, V_2 \rangle^\kappa\ \mathbf{in}\ M : \tau_3} \qquad \text{(T-Pair)}$$

We require $\kappa \neq \delta$ because there is no use creating a δ-value: since it can never be deallocated, creating a δ-value is the same as creating an ω-value.

Remark 3.6: Actually, annotating allocation of a pair with δ is meaningful and may be rather useful if the type τ_3 of M does not contain δ: we can modify the operational semantics so that $\mathbf{let}\ x = \langle V_1, V_2 \rangle^\delta\ \mathbf{in}\ M$ allocates the pair $\langle V_1, V_2 \rangle$ in the stack and deallocates it after M has been evaluated (recall that a value with use δ cannot be a part of the evaluation result).

The rule for the allocation of a closure is:

$$\frac{\Gamma_1, x : \tau_1 \vdash M_1 : \lceil \tau_2 \rceil \qquad \Gamma_2, f : \tau_1 \to^{\kappa_1, \kappa_2} \lceil \tau_2 \rceil \vdash M_2 : \tau_3 \qquad \kappa_1 \neq \delta}{\kappa_2 \lceil \Gamma_1 \rceil + \Gamma_2 \vdash \mathbf{let}\ f = \lambda^{\kappa_1} x.M_1\ \mathbf{in}\ M_2 : \tau_3} \qquad \text{(T-Abs)}$$

$\lceil \tau_2 \rceil$ in the premise $\Gamma_1, x : \tau_1 \vdash M_1 : \lceil \tau_2 \rceil$ guarantees that when the closure $\lambda x.M$ is called, it does not return a δ-value as a result. $\Gamma_1, x : \tau_1 \vdash M_1 : \lceil \tau_2 \rceil$ also means that during each call of the closure,

heap values are accessed as described by Γ_1. Because the other premise means that the closure will be called κ_2 times, the total access to heap values by M_1 can be represented by κ_2 copies of Γ_1, which is written as $\kappa_2\Gamma_1$. Since the access happens only later (not when $\lambda x.M_1$ is evaluated and the closure is created), $\lceil_\rceil$ is applied to it, so that it does not contain δ-values.

The following rule for recursive functions is similar to (T-Abs) except for the estimation of the use of the created function:

$$\frac{\Gamma_1, x : \tau_1, f : \tau_1 \to^{\kappa_1,\kappa_2} \lceil\tau_2\rceil \vdash M_1 : \lceil\tau_2\rceil \qquad \Gamma_2, f : \tau_1 \to^{\kappa_3,\kappa_4} \lceil\tau_2\rceil \vdash M_2 : \tau_3}{\kappa_4(1+\kappa_2)\lceil\Gamma_1\rceil + \Gamma_2 \vdash \mathbf{let}\ f = \mathbf{rec}^{\lceil\kappa_3(1+\kappa_1)\rceil}(f, x, M_1)\ \mathbf{in}\ M_2 : \tau_3} \quad \text{(T-Rec)}$$

The total number of calls of the function f is calculated by using the number κ_2 of calls in M_1 and the number κ_4 of calls in M_2. Since each invocation of f may result in other κ_2 invocations of f, the total calls are counted as $\kappa_4(1 + \kappa_2 + \kappa_2^2 + \cdots) = \kappa_4(1 + \kappa_2)$. The use of function f itself (in the relaxed sense) is similarly calculated by using its uses κ_1 and κ_3 in M_1 and M_2. The ceiling function $\lceil_\rceil$ is applied to $\kappa_1(1 + \kappa_3)$ just to make sure that the use is not δ.

3.4.3 Let-expressions

The following rule for let-expressions best illustrates how the evaluation order is taken into account in our type system:

$$\frac{\Gamma_1 \vdash M_1 : \lceil\tau_1\rceil \qquad \Gamma_2, x : \lceil\tau_1\rceil \vdash M_2 : \tau}{\Gamma_1;\Gamma_2 \vdash \mathbf{let}\ x = M_1\ \mathbf{in}\ M_2 : \tau} \quad \text{(T-Let)}$$

Here, the premise means that heap values are accessed by M_1 as described by Γ_1 and by M_2 as described by $\Gamma_2, x : \lceil\tau_1\rceil$. In ordinary linear type systems, the total use of heap values in $\mathbf{let}\ x = M_1\ \mathbf{in}\ M_2$ was computed by adding Γ_1 and Γ_2. However, since M_2 is evaluated only after M_1 has been fully evaluated, we estimate the total access of heap values by *sequential composition* $\Gamma_1;\Gamma_2$. So, if $\Gamma_1 = x : int \times^{\delta} int$ and $\Gamma_2 = x : int \times^{1} int$, then the total use is calculated as $\Gamma_1;\Gamma_2 = x : int \times^{\delta;1} int = x : int \times^{1} int$, although x may be accessed many times. We require the type of M_1 not to contain δ at top-level (by applying $\lceil_\rceil$ to τ_1), in order to make sure that every δ-value represented by Γ_1 is really "used up" during the evaluation of M_1 and does not escape to the rest of computation.

3.4.4 Access to heap values

The following is the rule for closure invocation:

$$\frac{\Gamma, x : \tau_1 \vdash M : \tau_2 \qquad \kappa > 0}{(f : \tau_3 \to^{\kappa,1} \tau_1 + V : \tau_3); \Gamma \vdash \mathbf{let}\ x = apply^{\kappa}(f, V)\ \mathbf{in}\ M : \tau_2} \quad \text{(T-App)}$$

The access to heap values by $apply^{\kappa}(f, V)$ is estimated as $f : \tau_3 \to^{\kappa,1} \tau_1 + V : \tau_3$. Note that the first use κ of the type of f should not be zero, and that the second use is 1, since the function is used once here. The access of heap values except for x by M is estimated as Γ. Since $apply^{\kappa}(f, V)$ is evaluated *before* M is evaluated, the total access can be estimated as their sequential composition $(f : \tau_3 \to^{\kappa,1} \tau_1 + V : \tau_3); \Gamma$.

The rule for reading the first element of a pair is:

$$\frac{\Gamma, y : \tau_1', x : \tau_1 \times^{\kappa'} \tau_2 \vdash M : \tau_3 \qquad \kappa > 0}{\Gamma, x : (\tau_1 + \tau_1') \times^{\kappa;\kappa'} \tau_2 \vdash \mathbf{let}\ y = \mathbf{fst}^{\kappa}(x)\ \mathbf{in}\ M : \tau_3} \quad \text{(T-Fst)}$$

The premise implies that the pair is used as a κ'-value in M *after* being used as a κ-value in $\mathbf{fst}^{\kappa}(x)$. So, the total use of x is estimated as $\kappa; \kappa'$. The first element may be accessed through either y or x, hence the total use of the first element is estimated as $\tau_1 + \tau_1'$.

Similarly, the rule for extraction of the second element of the pair is:

$$\frac{\Gamma, y : \tau_2', x : \tau_1 \times^{\kappa'} \tau_2 \vdash M : \tau_3 \qquad \kappa > 0}{\Gamma, x : \tau_1 \times^{\kappa;\kappa'} (\tau_2 + \tau_2') \vdash \mathbf{let}\ y = \mathbf{snd}^{\kappa}(x)\ \mathbf{in}\ M : \tau_3} \quad \text{(T-Snd)}$$

3.4.5 Rules for conditionals

In the following rule for conditional expressions, we require that the then-part and the else-part has the same typing.

$$\frac{\Gamma \vdash M_1 : \tau_1 \qquad \Gamma \vdash M_2 : \tau_1}{V : int + \Gamma \vdash \mathbf{if0}\ V\ \mathbf{then}\ M_1\ \mathbf{else}\ M_2 : \tau_1} \quad \text{(T-If)}$$

Example 3.7: A type judgment

$$\emptyset \vdash \mathbf{let}\ x = \langle 1, 2 \rangle^1\ \mathbf{in\ let}\ y = \mathbf{fst}^{\delta}(x)\ \mathbf{in\ let}\ z = \mathbf{snd}^1(x)\ \mathbf{in}\ z : int$$

is obtained from the following derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{z : int \vdash z : int}{x : int \times^0 int, y : int, z : int \vdash z : int}\ \text{(T-Weak)}}{x : int \times^1 int, y : int \vdash \mathbf{let}\ z = \mathbf{snd}^1(x)\ \mathbf{in}\ z : int}\ \text{(T-Snd)}}{x : int \times^1 int \vdash \mathbf{let}\ y = \mathbf{fst}^{\delta}(x)\ \mathbf{in\ let}\ z = \mathbf{snd}^1(x)\ \mathbf{in}\ z : int}\ \text{(T-Fst)}}{\emptyset \vdash \mathbf{let}\ x = \langle 1, 2 \rangle^1\ \mathbf{in\ let}\ y = \mathbf{fst}^{\delta}(x)\ \mathbf{in\ let}\ z = \mathbf{snd}^1(x)\ \mathbf{in}\ z : int}\ \text{(T-Pair)}$$

Definition of $\kappa_1 + \kappa_2$

$\kappa_1 \backslash \kappa_2$	0	δ	1	ω
0	0	δ	1	ω
δ	δ	ω	ω	ω
1	1	ω	ω	ω
ω	ω	ω	ω	ω

Definition of $\kappa_1 ; \kappa_2$

$\kappa_1 \backslash \kappa_2$	0	δ	1	ω
0	0	δ	1	ω
δ	δ	δ	1	ω
1	1	ω	ω	ω
ω	ω	ω	ω	ω

Definition of $\kappa_1 \cdot \kappa_2$

$\kappa_1 \backslash \kappa_2$	0	δ	1	ω
0	0	0	0	0
δ	0	δ	δ	ω
1	0	δ	1	ω
ω	0	ω	ω	ω

Definition of $\lceil \kappa \rceil$

κ	0	δ	1	ω
$\lceil \kappa \rceil$	0	1	1	ω

Definition of $\lfloor \kappa \rfloor$

κ	0	δ	1	ω
$\lfloor \kappa \rfloor$	0	0	1	ω

Figure 3: Operations on uses

4 Type Soundness

In this section, we show the type soundness property that no invalid heap access occurs during evaluation of well-typed expressions. The type soundness is formally stated as follows:

Theorem 4.1: If $\emptyset \vdash M : \tau$, then $(\{\}, M) \not\rightsquigarrow^* \textbf{Error}$.

We want to show this property as usual [8, 21], by defining a typing system for a run-time state (H, M) and proving that the reduction relation preserves typing and that no well-typed state (H, M) causes an error immediately. Unfortunately, however, the reduction relation $\rightsquigarrow$ defined in Section 2.3 is not suitable for this purpose: a key feature of our type system is to capture information on the order of heap access (recall (T-Let), for example), whereas the flat representation of a heap loses that information. Therefore, we define an alternative operational semantics that represents a heap by using nested letrec-expressions, and show the soundness of the type system with respect to that semantics. Although it includes rather strange reduction rules, it is easy to see that the alternative semantics is essentially equivalent to the original semantics.

In Section 4.1, we define the alternative semantics and show a theorem that intuitively says: (1) there is a correspondence between the reduction in the ordinary semantics and that in the alternative

Relation $\leq$

$$
\begin{array}{l}
int \leq int \\
(\tau_1 \times^{\kappa} \tau_2) \leq (\tau_1' \times^{\kappa'} \tau_2') \text{ if } (\tau_1 \leq \tau_1' \wedge \tau_2 \leq \tau_2' \wedge \kappa \leq \kappa') \\
(\tau_1 \rightarrow^{\kappa_1,\kappa_2} \tau_2) \leq (\tau_1 \rightarrow^{\kappa_1',\kappa_2'} \tau_2) \text{ if } (\kappa_1 \leq \kappa_1' \wedge \kappa_2 \leq \kappa_2') \\
\Gamma \leq \Gamma' \text{ if } dom(\Gamma) \subseteq dom(\Gamma') \text{ and } \Gamma(x) \leq \Gamma'(x) \text{ for each } x \in dom(\Gamma).
\end{array}
$$

Binary operations ($\mathbf{op} = +, ;$)

$$
\begin{array}{rcl}
int \mathbf{op} int & = & int \\
(\tau_1 \times^{\kappa} \tau_2)\mathbf{op}(\tau_1' \times^{\kappa'} \tau_2') & = & \begin{cases} (\tau_1 \mathbf{op} \tau_1') \times^{\kappa \mathbf{op} \kappa'} (\tau_2 \mathbf{op} \tau_2') \\ \qquad \text{if } \tau_1 \mathbf{op} \tau_1' \text{ and } \tau_2 \mathbf{op} \tau_2' \text{ are well defined.} \\ \text{undefined} \qquad \text{otherwise} \end{cases} \\
(\tau_1 \rightarrow^{\kappa_1,\kappa_2} \tau_2)\mathbf{op}(\tau_1 \rightarrow^{\kappa_1',\kappa_2'} \tau_2) & = & \tau_1 \rightarrow^{\kappa_1 \mathbf{op} \kappa_1', \kappa_2 \mathbf{op} \kappa_2'} \tau_2 \\
(\Gamma_1 \mathbf{op} \Gamma_2)(x) & = & \begin{cases} \Gamma_1(x)\mathbf{op}\Gamma_2(x) & \text{if } x \in dom(\Gamma_1) \cap dom(\Gamma_2) \\ \Gamma_1(x) & \text{if } x \in dom(\Gamma_1) \backslash dom(\Gamma_2) \\ \Gamma_2(x) & \text{if } x \in dom(\Gamma_2) \backslash dom(\Gamma_1) \end{cases}
\end{array}
$$

Unary operations ($\mathbf{op} = \lceil _ \rceil, \kappa \cdot _, \lfloor _ \rfloor$)

$$
\begin{array}{rcl}
\mathbf{op}(int) & = & int \\
\mathbf{op}(\tau_1 \times^{\kappa} \tau_2) & = & \mathbf{op}(\tau_1) \times^{\mathbf{op}(\kappa)} \mathbf{op}(\tau_2) \\
\mathbf{op}(\tau_1 \rightarrow^{\kappa_1,\kappa_2} \tau_2) & = & \tau_1 \rightarrow^{\mathbf{op}(\kappa_1),\mathbf{op}(\kappa_2)} \tau_2 \\
(\mathbf{op}(\Gamma))(x) & = & \mathbf{op}(\Gamma(x))
\end{array}
$$

Figure 4: Definitions of a relation and operations on types and type environments

semantics, and (2) if an expression is reduced to **Error** in the ordinary semantics, then it is also reduced to **Error** in the alternative semantics. These properties imply that if an expression is not reduced to **Error** in the alternative semantics, then it is not either in the ordinary semantics and the result of evaluation is the same. Section 4.5 is devoted to showing that no well-typed expression indeed is reduced to **Error** in the alternative semantics.

4.1 Alternative Operational Semantics

Before presenting the alternative semantics, we explain why the reduction relation $\rightsquigarrow$ fails to preserve typing. Let us consider the following configuration:

$$(\{w \mapsto^1 \langle 1, 2\rangle, x \mapsto^1 \langle w, 3\rangle\}, \mathbf{let}\ v = M_1\ \mathbf{in}\ M_2).$$

where $M_1 = \mathbf{let}\ y = \mathbf{fst}^\delta(x)\ \mathbf{in}\ \mathbf{let}\ z = \mathbf{fst}^\delta(y)\ \mathbf{in}\ z$. Then, $x : (\mathit{int} \times^\delta \mathit{int}) \times^\delta \mathit{int} \vdash M_1 : \mathit{int}$. So, if $x : (\mathit{int} \times^1 \mathit{int}) \times^1 \mathit{int} \vdash M_2 : \mathit{int}$, then by (T-Let),

$$x : (\mathit{int} \times^1 \mathit{int}) \times^1 \mathit{int} \vdash \mathbf{let}\ v = M_1\ \mathbf{in}\ M_2 : \mathit{int},$$

since $((\mathit{int} \times^\delta \mathit{int}) \times^\delta \mathit{int}); ((\mathit{int} \times^1 \mathit{int}) \times^1 \mathit{int}) = (\mathit{int} \times^1 \mathit{int}) \times^1 \mathit{int}$. So it is fine that w is a linear pair. However, if we reduce the configuration by (R-Fst), the resulting configuration:

$$(\{w \mapsto^1 \langle 1, 2\rangle, x \mapsto^1 \langle w, 3\rangle\}, \mathbf{let}\ v = (\mathbf{let}\ z = \mathbf{fst}^\delta(w)\ \mathbf{in}\ z)\ \mathbf{in}\ M_2)$$

requires w to be an ω-pair: w is accessed as a linear pair in M (through x) and as a δ-pair in $\mathbf{fst}^\delta(w)$, and the type system cannot capture the order between the two uses (because the access is made through different variables x and w).

One way to avoid the above problem would be to extend the type system so that the order of access to different variables can be expressed, as in [11]. Since the resulting typing rules would become rather complex, we instead redefine the operational semantics. The idea is, before losing information on the order of heap access, to split the heap space in advance by taking the order into account. For example, the above configuration is first converted to something like:

$$\begin{array}{l}\mathbf{let}\ v = (\{w \mapsto^\delta \langle 1, 2\rangle, x \mapsto^\delta \langle w, 3\rangle\}, M_1)\\ \mathbf{in}\ (\{w \mapsto^1 \langle 1, 2\rangle, x \mapsto^1 \langle w, 3\rangle\}, M_2).\end{array}$$

Since the heap space has been split for the definition part and for the body part of the let-expression, we can safely throw away information that the definition part is evaluated before the body part. So, it can be reduced to:

$$\begin{array}{l}\mathbf{let}\ v = (\{w \mapsto^\delta \langle 1, 2\rangle, x \mapsto^\delta \langle w, 3\rangle\}, \mathbf{let}\ z = \mathbf{fst}^\delta(w)\ \mathbf{in}\ z)\\ \mathbf{in}\ (\{w \mapsto^1 \langle 1, 2\rangle, x \mapsto^1 \langle w, 3\rangle\}, M_2).\end{array}$$

In order to express the above kinds of nested heap and expression, we introduce a new class of expressions called *dynamic expressions* in Section 4.2. We then define a reduction relation for dynamic expressions in Section 4.3 and discuss correspondence between the original semantics and the new semantics in Section 4.4.

Note that the new operational semantics is introduced just for proving Theorem 4.1. The actual implementation can be based on the semantics defined in Section 2.3 and no cost for splitting heap needs to be paid.

4.2 Dynamic expressions

The syntax of expressions given in Section 2 is extended to that of dynamic expressions as follows:

Definition 4.2 [dynamic expressions]: The set $\mathcal{D}$ of dynamic expressions, ranged over by D, is given by the following syntax:

$$D \ ::= \ M \mid \mathbf{let}\ x = D_1\ \mathbf{in}\ D_2 \mid \mathbf{letrec}\ x = h^{\kappa}\ \mathbf{in}\ D$$

Here, we introduced a letrec-expression $\mathbf{letrec}\ x = h^{\kappa}\ \mathbf{in}\ D$ to express a heap binding, and extended the syntax of let-expressions so that heap bindings and let-bindings can be nested. Unlike x in a let-expression $\mathbf{let}\ x = M_1\ \mathbf{in}\ M_2$, we regard x in a letrec-expression $\mathbf{letrec}\ x = h^{\kappa}\ \mathbf{in}\ D$ as a *free* variable.

By using the new syntax, the nested heap and expression

$$\mathbf{let}\ v = (\{x \mapsto^{\delta} \langle w, 3\rangle\}, M_1)\ \mathbf{in}\ (\{x \mapsto^{1} \langle w, 3\rangle\}, M_2)$$

can be expressed by the following dynamic expression:

$$\begin{array}{l}\mathbf{let}\ v = (\mathbf{letrec}\ x = \langle w, 3\rangle^{\delta}\ \mathbf{in}\ M_1)\\ \mathbf{in}\ \mathbf{letrec}\ x = \langle w, 3\rangle^{1}\ \mathbf{in}\ M_2\end{array}$$

Example 4.3:

$$\mathbf{letrec}\ x = \langle 1, 2\rangle^{\omega}\ \mathbf{in}\ \mathbf{letrec}\ f = \lambda^{1} y.(\mathbf{let}\ z = \mathbf{fst}^{1}(x)\ \mathbf{in}\ z)\ \mathbf{in}\ \mathbf{let}\ w = apply^{1}(f, 0)\ \mathbf{in}\ w$$

represents the configuration:

$$(\{x \mapsto^{\omega} \langle 1, 2\rangle, f \mapsto^{1} \lambda y.(\mathbf{let}\ z = \mathbf{fst}^{1}(x)\ \mathbf{in}\ z)\}, \mathbf{let}\ w = apply^{1}(f, 0)\ \mathbf{in}\ w).$$

Example 4.4: Heaps and expressions are nested in the following expression:

$$\mathbf{let}\ x = (\mathbf{letrec}\ y = \langle 1, 2\rangle^{\delta}\ \mathbf{in}\ \mathbf{let}\ z = \mathbf{fst}^{\delta}(y)\ \mathbf{in}\ z)\ \mathbf{in}\ \mathbf{letrec}\ y = \langle 1, 2\rangle^{1}\ \mathbf{in}\ \mathbf{let}\ w = \mathbf{snd}^{\delta}(y)\ \mathbf{in}\ w$$

It means that the expression to be evaluated is
$\mathbf{let}\ x = (\mathbf{let}\ z = \mathbf{fst}^{\delta}(y)\ \mathbf{in}\ z)\ \mathbf{in}\ \mathbf{let}\ w = \mathbf{snd}^{\delta}(y)\ \mathbf{in}\ w$, and when $\mathbf{let}\ z = \mathbf{fst}^{\delta}(y)\ \mathbf{in}\ z$ is evaluated, y is viewed as a δ-value while it is viewed as a linear value when $\mathbf{let}\ w = \mathbf{snd}^{\delta}(y)\ \mathbf{in}\ w$ is evaluated.

4.3 Operational semantics of dynamic expressions

We define an operational semantics by using a reduction relation $D \xrightarrow{l} E$. D is a dynamic expression and E is either a dynamic expression or a special constant **Error** representing invalid heap access. The label l shows which heap value is accessed in the reduction step. It is either ϵ, which indicates that an internal heap value is accessed, or $x = h^\kappa$, which indicates that the heap address x is accessed as a value with use κ, or x, which indicates that the heap of address x is split as explained above.

The following two rules are for heap allocation, which correspond to the rules (R-Heap), and (R-Rec).

$$\textbf{let } x = h^\kappa \textbf{ in } M \xrightarrow{\epsilon} \textbf{letrec } z = h^\kappa \textbf{ in } [z/x]M \ (z \text{ fresh}) \tag{DR-Heap}$$

$$\textbf{let } y = \textbf{rec}^\kappa(f, x, M_1) \textbf{ in } M_2 \xrightarrow{\epsilon} \textbf{letrec } z = \lambda^\kappa x.[z/f]M_1 \textbf{ in } [z/y]M_2 \ (z \text{ fresh}) \tag{DR-Rec}$$

The following three rules are for heap access. A label is used to record which heap address was accessed as a value of which use.

$$\textbf{let } u = \textbf{fst}^\kappa(x) \textbf{ in } M \xrightarrow{x=\langle V_1, V_2\rangle^\kappa} [V_1/u]M \tag{DR-Fst}$$

$$\textbf{let } u = \textbf{snd}^\kappa(x) \textbf{ in } M \xrightarrow{x=\langle V_1, V_2\rangle^\kappa} [V_2/u]M \tag{DR-Snd}$$

$$\textbf{let } u = \mathit{apply}^\kappa(x, V) \textbf{ in } M' \xrightarrow{x=\lambda^\kappa z.M} \textbf{let } u = [V/z]M \textbf{ in } M' \tag{DR-App}$$

The following two rules check whether each heap access is valid or not. If the use κ of the heap value is less than the consumed use κ', then the access is invalid and therefore the expression is reduced to **Error**. Otherwise, the evaluation succeeds and the consumed use κ' is removed from κ.

$$\frac{D \xrightarrow{x=h^{\kappa'}} D' \qquad \kappa \geq \kappa' > 0}{\textbf{letrec } x = h^\kappa \textbf{ in } D \xrightarrow{\epsilon} \textbf{letrec } x = h^{\kappa-\kappa'} \textbf{ in } D'} \tag{DR-Read}$$

$$\frac{D \xrightarrow{x=h^{\kappa'}} D' \qquad (\kappa' > \kappa) \vee (\kappa' = 0)}{\textbf{letrec } x = h^\kappa \textbf{ in } D \xrightarrow{\epsilon} \textbf{Error}} \tag{DR-Error}$$

The followings are the rules for conditional expressions.

$$\textbf{if0 } 0 \textbf{ then } M_1 \textbf{ else } M_2 \xrightarrow{\epsilon} M_1 \tag{DR-IfT}$$

$$\frac{n \neq 0}{\textbf{if0}\ n\ \textbf{then}\ M_1\ \textbf{else}\ M_2 \xrightarrow{\epsilon} M_2} \quad \text{(DR-IfF)}$$

The following two rules specify which part of an expression can be evaluated. (DR-ConRec) says that if an expression can be reduced, it can also be reduced in the same way even when an irrelevant heap has been added. (DR-ConLet) says that, in a let-expression, the definition part should be reduced first.

$$\frac{D \xrightarrow{l} D' \qquad x \text{ does not appear in } l}{\textbf{letrec}\ x = h^{\kappa}\ \textbf{in}\ D \xrightarrow{l} \textbf{letrec}\ x = h^{\kappa}\ \textbf{in}\ D'} \quad \text{(DR-ConRec)}$$

$$\frac{D_1 \xrightarrow{l} D_1' \qquad l \text{ is } \epsilon \text{ or } y}{\textbf{let}\ x = D_1\ \textbf{in}\ D_2 \xrightarrow{l} \textbf{let}\ x = D_1'\ \textbf{in}\ D_2} \quad \text{(DR-ConLet)}$$

The following rules are for error propagation.

$$\frac{D_1 \xrightarrow{\epsilon} \textbf{Error}}{\textbf{let}\ x = D_1\ \textbf{in}\ D_2 \xrightarrow{\epsilon} \textbf{Error}} \quad \text{(DR-ErrLet)}$$

$$\frac{D \xrightarrow{\epsilon} \textbf{Error}}{\textbf{letrec}\ x = h^{\kappa}\ \textbf{in}\ D \xrightarrow{\epsilon} \textbf{Error}} \quad \text{(DR-ErrRec)}$$

The following rule (DR-Split) is a key rule. As explained above, before a let-expression is evaluated, a heap value is "split" into two: one for evaluation of the definition-part and the other for evaluation of the body-part.

$$\textbf{letrec}\ x = h^{\kappa_1;\kappa_2}\ \textbf{in let}\ y = D_1\ \textbf{in}\ D_2 \xrightarrow{x} \textbf{let}\ y = \textbf{letrec}\ x = h^{\kappa_1}\ \textbf{in}\ D_1\ \textbf{in letrec}\ x = h^{\kappa_2}\ \textbf{in}\ D_2 \quad \text{(DR-Split)}$$

If the definition-part of a let-expression has been fully evaluated, split heap values can be merged, with δ-values being thrown away.

$$\begin{aligned}\textbf{let}\ x = (\textbf{letrec}\ \vec{z} = \vec{h}^{\vec{\kappa_1}}\ \textbf{in letrec}\ \vec{w} = \vec{h'}^{\vec{\kappa_3}}\ \textbf{in}\ V)\ \textbf{in}\ (\textbf{letrec}\ \vec{z} = \vec{h}^{\vec{\kappa_2}}\ \textbf{in}\ M)\\ \xrightarrow{\epsilon} \textbf{letrec}\ \vec{z} = \vec{h}^{\lfloor\vec{\kappa_1}\rfloor;\vec{\kappa_2}}\ \textbf{in letrec}\ \vec{w} = \vec{h'}^{\lfloor\vec{\kappa_3}\rfloor}\ \textbf{in}\ [V/x]M\end{aligned} \quad \text{(DR-Var)}$$

Here, $\textbf{letrec}\ \vec{z} = \vec{h}^{\vec{\kappa}}\ \textbf{in}\ D$ is a shorthand for $\textbf{letrec}\ z_1 = h_1^{\kappa_1}\ \textbf{in} \cdots \textbf{letrec}\ z_n = h_n^{\kappa_n}\ \textbf{in}\ D$.

Example 4.5: The expression in Example 2.4 is reduced as follows:

$$
\begin{array}{ll}
 & \textbf{let } x = \langle 1,2\rangle^1 \textbf{ in let } y = \textbf{fst}^\delta(x) \textbf{ in let } z = \textbf{snd}^1(x) \textbf{ in } z \\
\xrightarrow{\epsilon} & \textbf{letrec } x = \langle 1,2\rangle^1 \textbf{ in let } y = \textbf{fst}^\delta(x) \textbf{ in let } z = \textbf{snd}^1(x) \textbf{ in } z \\
\xrightarrow{x} & \textbf{let } y = (\textbf{letrec } x = \langle 1,2\rangle^\delta \textbf{ in fst}^\delta(x)) \textbf{ in} \\
 & \quad (\textbf{letrec } x = \langle 1,2\rangle^1 \textbf{ in let } z = \textbf{snd}^1(x) \textbf{ in } z) \\
\xrightarrow{\epsilon} & \textbf{let } y = (\textbf{letrec } x = \langle 1,2\rangle^\delta \textbf{ in } 1) \textbf{ in} \\
 & \quad (\textbf{letrec } x = \langle 1,2\rangle^1 \textbf{ in let } z = \textbf{snd}^1(x) \textbf{ in } z) \\
\xrightarrow{\epsilon} & \textbf{letrec } x = \langle 1,2\rangle^{\delta;1} \textbf{ in let } z = \textbf{snd}^1(x) \textbf{ in } z \\
\xrightarrow{x} & \textbf{let } z = (\textbf{letrec } x = \langle 1,2\rangle^1 \textbf{ in snd}^1(x)) \textbf{ in } (\textbf{letrec } x = \langle 1,2\rangle^0 \textbf{ in } z) \\
\xrightarrow{\epsilon} & \textbf{let } z = (\textbf{letrec } x = \langle 1,2\rangle^0 \textbf{ in } 2) \textbf{ in } (\textbf{letrec } x = \langle 1,2\rangle^0 \textbf{ in } z) \\
\xrightarrow{\epsilon} & \textbf{letrec } x = \langle 1,2\rangle^0 \textbf{ in } 2
\end{array}
$$

4.4 Correspondence between the heap-based operational semantics and the alternative operational semantics

Although the alternative operational semantics given above may look strange, it is essentially equivalent to the heap-based operational semantics. Basically, each rule (DR-XX) corresponds to (R-XX), and the rules (DR-Read), (DR-ConRec) and (DR-ConLet) are introduced instead of using context $C[\ ]$. So, the only special rules are (DR-Split) and (DR-Var). The role of (DR-Split) is just to force the access capability of each heap value to be split into two; so, it may causes more errors (due to inappropriate splitting), but it does not change the result of a successful evaluation. We formally state it in Theorem 4.8 below, after introducing several definitions.

Definition 4.6 [translation of dynamic expressions]: A translation function $(_)^* \in \mathcal{D} \to (\mathcal{H} \times \mathcal{E})$ is defined by:

$$
\begin{array}{rcl}
V^* & = & (\{\}, V) \\
(\textbf{let } x = h^\kappa \textbf{ in } M)^* & = & (\{\}, \textbf{let } x = h^\kappa \textbf{ in } M) \\
(\textbf{let } x = \textbf{rec}^\kappa(f,y,M_1) \textbf{ in } M_2)^* & = & (\{\}, \textbf{let } x = \textbf{rec}^\kappa(f,y,M_1) \textbf{ in } M_2) \\
(\textbf{let } x = \textbf{fst}^\kappa(y) \textbf{ in } M)^* & = & (\{\}, \textbf{let } x = \textbf{fst}^\kappa(y) \textbf{ in } M) \\
(\textbf{let } x = \textbf{snd}^\kappa(y) \textbf{ in } M)^* & = & (\{\}, \textbf{let } x = \textbf{snd}^\kappa(y) \textbf{ in } M) \\
(\textbf{let } x = \mathit{apply}^\kappa(y,V) \textbf{ in } M)^* & = & (\{\}, \textbf{let } x = \mathit{apply}^\kappa(y,V) \textbf{ in } M) \\
(\textbf{if0 } V \textbf{ then } M_1 \textbf{ else } M_2)^* & = & (\{\}, \textbf{if0 } V \textbf{ then } M_1 \textbf{ else } M_2) \\
(\textbf{let } x = D_1 \textbf{ in } D_2)^* & = & (H_1; H_2, \textbf{let } x = M_1 \textbf{ in } M_2) \\
 & & \quad \text{where } (H_1, M_1) = D_1^* \wedge (H_2, M_2) = D_2^* \\
(\textbf{letrec } x = h^\kappa \textbf{ in } D)^* & = & (\{x \mapsto^\kappa h\} + H, M) \text{ where } (H, M) = D^*
\end{array}
$$

where $H_1; H_2$ and $H_1 + H_2$ are defined by:

$$(H_1; H_2)(x) = \begin{cases} (\kappa_1; \kappa_2, h) & \text{if } H_1(x) = (\kappa_1, h) \text{ and } H_2(x) = (\kappa_2, h) \\ H_1(x) & \text{if } x \in dom(H_1) \text{ and } x \notin dom(H_2) \\ H_2(x) & \text{if } x \in dom(H_2) \text{ and } x \notin dom(H_1) \end{cases}$$

$$(H_1 + H_2)(x) = \begin{cases} H_2(x) & \text{if } x \in dom(H_2) \\ H_1(x) & \text{if } x \in dom(H_1) \text{ and } x \notin dom(H_2) \end{cases}$$

Definition 4.7: The binary relation $\geq$ on heaps is defined by:

$$\begin{aligned} H_1 \geq H_2 \iff & (dom(H_1) = dom(H_2)) \\ & \wedge \forall x, \kappa_1, \kappa_2, h_1, h_2.((H_1(x) = (\kappa_1, h_1) \wedge H_2(x) = (\kappa_2, h_2)) \Rightarrow (h_1 = h_2 \wedge \kappa_1 \geq \kappa_2)). \end{aligned}$$

We write $(H_1, M_1) \geq (H_2, M_2)$ if $M_1 \equiv M_2$ and $H_1 \geq H_2$.

The correspondence between the new semantics and the heap-based semantics in Section 2 is formally stated in the theorem below. Intuitively, it means (1) the new semantics and the heap-based semantics are equivalent as long as no error occurs, and (2) if an error occurs in the heap-based semantics, so in the new semantics (the converse may not hold).

We write $D \xrightarrow{\hat{\epsilon}} D'$ if $D \xrightarrow{x_1} \cdots \xrightarrow{x_n} \xrightarrow{\epsilon} D'$ for some $x_1, \ldots, x_n$. We also write $D \uparrow$ if D is reduced to **Error** no matter how the heap bindings in D are split, i.e., if $D \xrightarrow{\hat{\epsilon}}$ **Error** and there is no $D' \in \mathcal{D}$ such that $D \xrightarrow{\hat{\epsilon}} D'$. Here, we restrict the syntax of dynamic expressions so that, if D contains an expression of the form **let** $x = D$ **in letrec** $\vec{x} = \vec{h}^{\vec{\kappa}}$ **in** M, then D is of the form **letrec** $\vec{x} = \vec{h}^{\vec{\kappa'}}$ **in letrec** $\vec{y} = \vec{h'}^{\vec{\kappa''}}$ **in** M' and $\vec{y}$ do not appear in M. We also require that there is no forward reference, i.e., if $D =$ **letrec** $x = h^{\kappa}$ **in** D_1 and h contains free occurrences of y, then D_1 does not contain a sub-expression of the form **letrec** $y = h'^{\kappa'}$ **in** D_2.

Theorem 4.8:

1. If $D \xrightarrow{\hat{\epsilon}} D'$, then $D^* \rightsquigarrow (H, M)$ and $(H, M) \geq D'^*$ for some H, M.
2. If $(H, M) \rightsquigarrow$ **Error** and $(H, M) \geq D^*$, then $D \uparrow$.
3. If $(H, M) \rightsquigarrow (H', M')$ and $(H, M) \geq D^*$, then either $D \uparrow$ or there exists D' such that $D \xrightarrow{\hat{\epsilon}} D'$ and $(H', M') \geq D'^*$.

Proof: See Appendix A.4. □

4.5 Type Soundness

Since we have checked the correspondence between the new operational semantics and the original one above, we can obtain Theorem 4.1 by showing soundness of the type system with respect to the new semantics. We show it by proving that reductions in the alternative semantics preserve typing and that no well-typed expression accesses an invalid heap address immediately. We extend the type system for dynamic expressions by introducing the following rules:

$$\frac{x \notin \{V_1, V_2\}}{V_1 : \tau_1 + V_2 : \tau_2 \vdash x = \langle V_1, V_2 \rangle^{\kappa} : \tau_1 \times^{\kappa} \tau_2} \quad \text{(DT-Pair)}$$

$$\frac{\Gamma_1, x : \tau_1, f : \tau_1 \to^{\kappa_1, \kappa_2} \lceil \tau_2 \rceil \vdash M_1 : \tau_2 \qquad \kappa \geq \kappa_3(1 + \kappa_1)}{\kappa_4(1 + \kappa_2)\lceil \Gamma_1 \rceil \vdash f = \lambda^{\kappa} x.M_1 : \tau_1 \to^{\kappa_3, \kappa_4} \lceil \tau_2 \rceil} \quad \text{(DT-Abs)}$$

$$\frac{\Gamma_1 \vdash x = h^{\kappa} : \tau_1 \qquad \Gamma_2, x : \tau_1 \vdash D : \tau_2}{\Gamma_1 + \Gamma_2 \vdash \textbf{letrec } x = h^{\kappa} \textbf{ in } D : \tau_2} \quad \text{(DT-Heap)}$$

The type soundness is guaranteed by the two theorems below. Proofs are given in Appendix A.

Theorem 4.9: If $\Gamma \vdash D : \tau$, then $D \not\xrightarrow{\epsilon}$ **Error**.

Theorem 4.10 [Subject Reduction]:

- If $\Gamma \vdash D : \tau$ and $D \xrightarrow{\epsilon} D'$, then $\Gamma \vdash D' : \tau$; and
- If $\Gamma \vdash D : \tau$ and $D \xrightarrow{x} D'$, then there exists D'' such that $D \xrightarrow{x} D''$ and $\Gamma \vdash D'' : \tau$.

The above subject reduction property is a little more complicated than the usual one because even a well-typed dynamic expression may be reduced to an ill-typed expression if a heap value is split in an inappropriate way. For example, **letrec** $x = \langle 1, 2 \rangle^1$ **in let** $z = \textbf{snd}^1(x)$ **in** z can be reduced by (DR-Split) to **let** $z = (\textbf{letrec } x = \langle 1, 2 \rangle^{\delta} \textbf{ in } \textbf{snd}^1(x))$ **in** $(\textbf{letrec } x = \langle 1, 2 \rangle^1 \textbf{ in } z)$, which is not well typed and will be reduced to **Error**. The second statement of the lemma says that, if heap splitting (the rule (DR-Split)) can be applied to a well-typed expression, there is always a *good* splitting that preserves the well-typeness of the expression.

The type soundness (Theorem 4.1) follows immediately from the above theorems.

Proof of Theorem 4.1: Suppose $\emptyset \vdash M : \tau$ and $(\{\}, M)(= (H_0, M_0)) \rightsquigarrow (H_1, M_1) \rightsquigarrow \cdots \rightsquigarrow (H_n, M_n) \rightsquigarrow$ **Error**. By Theorem 4.8 and Theorem 4.10, there are k and D such that $0 \leq k \leq n$, $M \longrightarrow^* D$, $\emptyset \vdash D : \tau$, $(H_k, M_k) \geq D^*$, and $D \uparrow$. $\emptyset \vdash D : \tau$ and $D \uparrow$ contradict with Theorem 4.9 and Theorem 4.10. □

5 Type Reconstruction

Use annotations can be automatically inferred from unannotated expressions. Since it is done basically in the same way as that for previous linear type systems [9, 21], we explain it only informally. The basic idea is to introduce variables ranging over uses and types, and constraints on them, so that we can express the most general typing (principal typing) of an expression. A new type judgment is of the form $\Gamma, C \vdash M : \tau$, where a set of constraints C specifies which set of uses/types each use/type variable (in Γ, M, or τ) can range over. For instance, $\mathbf{let}\ x = \langle y, y\rangle\ \mathbf{in}\ x$ is typed as: $y : \alpha, \{\alpha \geq \beta + \gamma, i \neq \delta, i \geq j\} \vdash \mathbf{let}\ x = \langle y, y\rangle^i\ \mathbf{in}\ x : \beta \times^j \gamma$. This typing is *principal* in the sense that all the typings derivable from the rules in Section 3 can be obtained by instantiating variables α, β, γ, i and j so that the constraint is satisfied. (We do not give the formal definition of principal typings here; it is basically the same as that in [21].)

Given an unannotated expression M, the inference of a use annotation proceeds as follows (actually, the second and third steps may overlap):

1. Attach a fresh use variable to each place where use annotation is required (let the annotated expression be M').
2. Compute a principal typing $\Gamma, C \vdash M' : \tau$.
3. Solve the constraint C and apply the obtained substitution to M'.

In the following subsections, we explain the second and third steps in a little more detail, and then discuss the cost of the analysis.

5.1 Computing a principal typing

An algorithm for computing a principal typing is obtained by constructing syntax-directed typing rules for the new type judgment form and by reading them from bottom to up. For example, we can merge the rules (T-Pair) and (T-Weak) and obtain the following rule for the new type judgment form:

$$\frac{\begin{array}{c}\Gamma, x : \tau_1 \times^\kappa \tau_2, C \vdash M : \tau_3 \\ C \models \Gamma' \geq (\Gamma + V_1 : \tau_1 + V_2 : \tau_2) \\ C \models \kappa \neq \delta\end{array}}{\Gamma', C \vdash \mathbf{let}\ x = \langle V_1, V_2\rangle^\kappa\ \mathbf{in}\ M : \tau_3} \qquad \text{(TR-Pair)}$$

Here, $C \models \Gamma_1 \geq \Gamma_2$ means that, for any substitution θ on type/use variables, if θC is satisfied then $\theta\Gamma_1 \geq \theta\Gamma_2$ is also satisfied. The above rule says that in order to compute a typing for

let $x = \langle V_1, V_2 \rangle^\kappa$ **in** M, we should first compute a typing for M and then add new constraints entailing $\Gamma' \geq \Gamma + V_1 : \tau_1 + V_2 : \tau_2$ and $\kappa \neq \delta$.

One major difference from the previous linear type inference [8, 21] is that constraints on type variables appear in C (recall the typing for **let** $x = \langle y, y \rangle$ **in** x given above). They are of the form $\tau_1 \geq \tau_2$ or $\tau_1 \sim \tau_2$ (meaning τ_1 and τ_2 are *compatible* in the sense that $\tau_1 + \tau_2$ and $\tau_1; \tau_2$ are well defined; in other words, τ_1 and τ_2 are identical except for their outer uses). Here, the righthand type expression τ_2 of $\tau_1 \geq \tau_2$ may contain $+$, $\lceil _ \rceil$, etc. as constructors of type expressions (rather than as functions on types).

5.2 Solving constraints on types and uses

An algorithm for solving constraints can be divided into two steps. First, a set of constraints on type/use variables can be simplified into a pair of a set of constraints on use variables of the form $i \geq \kappa$[3] and a set of "trivial" constraints on type variables of the form $\alpha \sim \beta$ or $\alpha \geq \tau$ where τ is a type expression (such as $\beta + \gamma$) constructed only from type variables. This simplification is performed by *partial* unification of types, with some uses being kept different. For example, given a constraint $\alpha \geq (\beta \times^j \mathit{real}^i) + \gamma$, we can instantiate α and γ with $\beta' \times^{j'} \mathit{real}^{i'}$ and $\beta'' \times^{j''} \mathit{real}^{i''}$ for fresh variables $\beta', \beta'', i', i'', j', j''$ and reduce the constraint to $\{\beta' \geq \beta + \beta'', i' \geq i + i'', j' \geq j + j''\}$.

Next, since the set of trivial constraints on type variables always has a solution (let all the remaining type variables be instantiated with, say, *int*), we can obtain the least assignment to use variables by solving the set of constraints on use variables. We can use the simple iterative method used in previous linear type systems [8, 9]. Of course, the least assignment to some use variables cannot be completely determined until the whole program is given. For example, given an expression of type real^i, we cannot find the least assignment to the use variable i until we know all the places where the evaluation result of the expression is used. For these unknown variables, we can either simply assign ω or delay constraint solving.

One important difference from the previous linear type inference is that the least solution is not necessarily the best solution from the viewpoint of memory management. For example, consider an expression **let** $y = \langle 1, 2 \rangle$ **in** (**let** $x = \mathbf{fst}(y)$ **in** x). The least annotation is **let** $y = \langle 1, 2 \rangle^1$ **in** (**let** $x = \mathbf{fst}^\delta(y)$ **in** x). In this expression, y cannot be deallocated since the only access to the pair y ($\mathbf{fst}(y)$) is annotated with δ. Therefore, it is better to annotate the expression as **let** $y = \langle 1, 2 \rangle^1$ **in** (**let** $x = \mathbf{fst}^1(y)$ **in** x). We can think of two ways for dealing with this. One way is to classify uses into those for annotating heap allocation and those for annotating heap access. After the least solution is obtained, we can maximize heap access annotations as long as no heap allocation annotations increase. The other way is to extend a target language with an explicit deallocation operation *free*(Γ): It deallocates heap values as if the heap were accessed as described by Γ. For

[3] Note that a constraint $i \neq \delta$ can be expressed as $i \geq \lceil i \rceil$.

example, $\mathit{free}(x : \mathit{real}^1, y : \mathit{real}^\delta)$ deallocates x but not y. The rule (T-Weak) can be changed as follows ($\Gamma - \Gamma'$ is the least type environment Γ'' such that $\Gamma'; \Gamma'' = \Gamma$):

$$\frac{\Gamma' \vdash M : \tau \qquad \Gamma' \leq \Gamma}{\Gamma \vdash M; \mathit{free}(\Gamma - \Gamma') : \tau} \qquad \text{(T-Weak')}$$

This change avoids forgetting to deallocate linear values. We can optimize the result by moving the operation *free* leftward and merging it with heap access annotation as far as possible. Although there is no guarantee that these methods give the *best* use annotation, we expect that both give enough good an annotation in practice.

5.3 Cost of the analysis

Unfortunately, the computational cost for type reconstruction can be exponential in the size of an input in the worst case. The reason is that the number of use variables can be linear in the size of the type of a variable appearing in an input expression and that the size of a type can be exponential in the size of an input expression. For example, if a variable x is required to have type $(\mathit{int} \times \mathit{int}) \times (\mathit{int} \times \mathit{int})$ by the context, its typing is:

$$x : (\mathit{int} \times^{i_1} \mathit{int}) \times^{i_3} (\mathit{int} \times^{i_2} \mathit{int}), \{i_1 \geq i'_1, i_2 \geq i'_2, i_3 \geq i'_3\} \vdash x : (\mathit{int} \times^{i'_1} \mathit{int}) \times^{i'_3} (\mathit{int} \times^{i'_2} \mathit{int}).$$

So, the number of use variables is linear in the size 3 of the type $(\mathit{int} \times \mathit{int}) \times (\mathit{int} \times \mathit{int})$. Next, consider an expression

$$\textbf{let } x_0 = 1 \textbf{ in let } x_1 = \langle x_0, x_0 \rangle \textbf{ in let } x_2 = \langle x_1, x_1 \rangle \textbf{ in } \cdots \textbf{let } x_n = \langle x_{n-1}, x_{n-1} \rangle \textbf{ in } x_n.$$

The size of the type of the expression is exponential in n.

In spite of the above fact, we expect that the reconstruction can be performed efficiently for realistic programs for the following reasons. First, the above problem occurs only when tuple or record types are extraordinarily nested; a huge flat tuple type expression $\mathit{int} \times \mathit{int} \times \cdots \times \mathit{int}$ or an arrow type expression $\tau_1 \to \tau_2$ do not cause such problems. Second, if the computational cost is really problematic for some programs, we can save the cost by sacrificing the accuracy of the analysis. For example, we can restrict the $+$ operator so that $(\tau_1 \times^\kappa \tau_2) + (\tau'_1 \times^{\kappa'} \tau'_2)$ is defined only if $\tau_1 = \tau'_1$ and $\tau_2 = \tau'_2$. This forces many type expressions to be shared and saves the time and space of the analysis (in fact, the previous analysis in [8, 9], which imposes a similar restriction, is performed in polynomial time for the monomorphic type system).

6 Extensions

We have so far considered a simply-typed λ-calculus with recursion and pairs. In this section, we discuss two kinds of extensions: one is to introduce polymorphism in order to improve the analysis, and the other is to introduce other kinds of data such as recursive data structures and reference cells.

6.1 Polymorphism

Because the type system presented in Section 3 is monomorphic in both uses and types, the analysis of (quasi-)linear values is often rough. Consider the following expression:

$$\begin{array}{c}\textbf{let } f = \lambda x.\langle x, x\rangle \textbf{ in let } z = \mathit{apply}(f, 2) \textbf{ in} \\ \textbf{let } w = \mathit{apply}(f, 3) \textbf{ in } M.\end{array}$$

If either z or w is used as an ω-value in M, the other is also forced to be an ω-value, because the code for the pair creation (i.e., the body of the function f) is shared.

In order to avoid the above problem, we can introduce polymorphism on uses. Then, f can be given a type $\forall i :: \{i \geq \lceil i \rceil\}.(\mathit{int} \to^{1,\omega} (\mathit{int} \times^{i} \mathit{int}))$ and the above expression can be annotated, for example, as

$$\begin{array}{c}\textbf{let } f = \Lambda^{1} i.\lambda x.\langle x, x\rangle^{i} \textbf{ in let } z = \mathit{apply}^{\delta}(f[1], 2) \textbf{ in} \\ \textbf{let } w = \mathit{apply}^{1}(f[\omega], 3) \textbf{ in } M.\end{array}$$

Here, uses are explicitly passed as parameters to polymorphic functions. The use 1 attached to Λ indicates that the use-polymorphic function f is accessed linearly.

In general, we need to introduce the following *constrained type scheme*:

Definition 6.1:

$$\begin{array}{l} c \text{ (atomic constraints)} ::= i \geq u \mid \alpha \geq \rho \mid \alpha \sim \beta \\ \rho ::= \alpha \mid \rho_1 + \rho_2 \mid \rho_1; \rho_2 \mid u \cdot \rho \mid \lceil \rho \rceil \\ u ::= i \mid 0 \mid \delta \mid 1 \mid \omega \mid u_1 + u_2 \mid u_1; u_2 \mid u_1 \cdot u_2 \mid \lceil u \rceil \\ C ::= \{c_1, \ldots, c_n\} \\ \sigma \text{ (type schemes)} ::= \tau \mid \forall \vec{\alpha}, \vec{i} :: C.\sigma \end{array}$$

A new rule for polymorphic let-expressions roughly looks like:

$$\frac{\begin{array}{c}\Gamma_1, C_1 \wedge C_2 \vdash M_1 : \lceil \tau_1 \rceil \qquad \Gamma_2, x : \forall \vec{\alpha}, \vec{i} :: C_2.\lceil \tau_1 \rceil, C_3 \vdash M_2 : \tau_2 \\ \vec{i}, \vec{\alpha} \notin \mathit{Cv}(\Gamma_1, C_1, C_2) \qquad \{\vec{i}, \vec{\alpha}\} \supseteq \mathit{DCv}(C_2)\end{array}}{\Gamma_1; \Gamma_2, C_1 \wedge C_3 \vdash \textbf{let } x = M_1 \textbf{ in } M_2 : \tau_2} \quad \text{(T-LetPoly)}$$

Here, $Cv(\Gamma, C_1, C_2)$ denotes the set of type/use variables that may influence the value of some type/use variable in Γ or C_1. It is the least set satisfying the following conditions:

$$(Fv(C_1) \cup Fv(\Gamma)) \subseteq Cv(\Gamma, C_1, C_2)$$
$$(\alpha \in Cv(\Gamma, C_1, C_2)) \wedge ((\alpha \geq \rho) \in C_2) \Rightarrow Fv(\rho) \subseteq Cv(\Gamma, C_1, C_2)$$
$$(\alpha \in Cv(\Gamma, C_1, C_2)) \wedge (((\alpha \sim \beta) \in C_2) \vee ((\beta \sim \alpha) \in C_2)) \Rightarrow \beta \in Cv(\Gamma, C_1, C_2)$$
$$(i \in Cv(\Gamma, C_1, C_2)) \wedge ((i \geq u) \in C_2) \Rightarrow Fv(u) \subseteq Cv(\Gamma, C_1, C_2)$$

where $Fv(\Gamma), Fv(C), Fv(\rho)$, and $Fv(u)$ denote the set of free type/use variables appearing in Γ, C, ρ, and u respectively. $DCv(C)$ denotes the set of type/use variables constrained by C; it is defined by

$$DCv(C) = \{\alpha, \beta \mid \alpha \sim \beta \in C\} \cup \{\alpha \mid \alpha \geq \tau \in C\} \cup \{i \mid i \geq u \in C\}.$$

Remark 6.2: In the actual implementation, we may need to allocate each instance ($f[1]$ and $f[2]$ in the above example) of a use-polymorphic function in the heap. In the above annotation, it is assumed that such instances are deallocated when the use-polymorphic function is deallocated. In order to deallocate each instance of a use-polymorphic function separately, we need to annotate a type scheme with a use; for example, the type scheme of f should be changed to

$$\forall^1 i, j :: \{i \geq \lceil i \rceil, j \geq \lceil j \rceil\}.(int \rightarrow^{j,\omega} (int \times^i int)).$$

The above expression can be annotated as

$$\begin{array}{l} \textbf{let } f = \Lambda^1\langle i, j\rangle.\lambda^j x.\langle x, x\rangle^i \textbf{ in let } z = apply^1(f^\delta[1,1], 2) \textbf{ in} \\ \quad \textbf{let } w = apply^1(f^1[\omega, 1], 3) \textbf{ in } M. \end{array}$$

Here, the use annotation 1 in f^1 means that the polymorphic function f can be deallocated when the instance created there is deallocated. The use attached to *apply* represents whether the instance can be deallocated.

6.2 Large constants

So far, we have considered only integers as constants. In order to deal with large constants (i.e., constants that cannot be represented in one word and must be allocated in a heap), we need to annotate each allocation of a large constant. For example, allocation of a linear real number 2.0 is annotated as **let** $x = 2.0^1$ **in** $\cdots$. The type of a large constant is also annotated with a use. For instance, the type of linear real numbers is represented by $real^1$. The typing rule for real numbers is given as follows:

$$\frac{\Gamma, x : real^\kappa \vdash M : \tau}{\Gamma \vdash \textbf{let } x = r^\kappa \textbf{ in } M : \tau}$$

6.3 Primitive functions

Primitive functions can be treated as constants of polymorphic types, and each occurrence of a primitive function can be annotated with uses. For example, the primitive + on real numbers can be assigned a type

$$\forall i_1, i_2, i_3, i_4 :: \{i_1 \geq \delta, i_2 \geq \delta, i_3 \geq \delta, i_4 \geq \lceil i_4 \rceil\}.$$
$$((real^{i_1} \times^{i_3} real^{i_2}) \rightarrow^{\omega,\omega} real^{i_4}).$$

The expression **let** $x = y + z$ **in** $\cdots$ can be annotated like: **let** $x = +[1,1,1,1]\langle y, z\rangle^1$ **in** $\cdots$.

6.4 Recursive data structures

Recursive data structures such as lists and trees can be treated in the same way as pairs, by annotating their type constructors with uses. The type of a list of values of type τ is expressed as $\tau\ list^{\kappa}$, where κ expresses the use of each cons cell of the list. For example, $real^1\ list^{\omega}$ is the type of a list whose cons cells may be accessed many times in an arbitrary manner, but whose elements are real numbers that can be accessed only linearly. Primitives for lists can be given the following types:

$$\begin{array}{lcl}
:: & : & \forall \alpha, i.((\alpha \times^i \alpha\ list^i) \rightarrow^{\omega,\omega} \alpha\ list^i) \\
nil & : & \forall \alpha, i.\alpha\ list^i \\
null & : & \forall \alpha, i.(\alpha\ list^i \rightarrow^{\omega,\omega} bool) \\
hd & : & \forall \alpha, i :: \{i \geq \delta\}.(\alpha\ list^i \rightarrow^{\omega,\omega} \alpha) \\
tl & : & \forall \alpha, i :: \{i \geq \delta\}.(\alpha\ list^i \rightarrow^{\omega,\omega} \alpha\ list^i)
\end{array}$$

With these types, the function *append* is given the following type:

$$\forall \alpha, \beta, \gamma, i, j, k :: \{\alpha \geq \gamma, \beta \geq \gamma, i \geq \delta, j \geq k, j \geq \delta, k \geq \lceil k \rceil, l \geq \delta.((\alpha\ list^i \times^l \beta\ list^j) \rightarrow^{\omega,\omega} \gamma\ list^k).$$

In general, we can generate the types of constructors and destructors from datatype declarations of Standard ML [14].

6.5 Reference Cells

In order to deal with reference cells, we need to introduce a new type constructor. The type of a reference cell is of the form $\tau\ ref^{\kappa_1,\kappa_2}$, where τ is the type of a stored value, κ_1 is the use of the reference cell, and κ_2 denotes how many times each stored value may be read.

The primitives for reference cells are annotated as follows:

$$M ::= \cdots \mid \textbf{let } x = \textbf{ref}^{\kappa}(y) \textbf{ in } M \mid \textbf{let } x = !^{\kappa} y \textbf{ in } M \mid \textbf{let } x :=^{\kappa} V \textbf{ in } M$$

$\mathbf{ref}^\kappa(y)$ creates a reference cell x and store y into it; x can be accessed as a κ-value afterwards. $!^\kappa y$ reads the value stored in the reference cell y; at the same time, if κ is 1 and the reference y is linear, it deallocates the reference cell. $x :=^\kappa V$ stores the value V into the reference cell x; at the same time, if κ is 1 and the reference y is linear, it deallocates the reference cell.

Typing rules can be given, for example, as follows:

$$\frac{\Gamma, x : \lceil \tau \rceil \ \mathit{ref}^{\kappa_1,\kappa_2} \vdash M : \tau' \qquad \kappa_1 \neq \delta}{\Gamma + y : \kappa_2 \lceil \tau \rceil \vdash \mathbf{let}\ x = \mathbf{ref}^{\kappa_1}(y)\ \mathbf{in}\ M : \tau'} \quad \text{(T-Ref)}$$

$$\frac{\Gamma, y : \tau\ \mathit{ref}^{\kappa_1,\kappa_2}, x : \tau \vdash M : \tau' \qquad \kappa > 0}{\Gamma, y : \tau\ \mathit{ref}^{\kappa;\kappa_1,1+\kappa_2} \vdash \mathbf{let}\ x =!^\kappa y\ \mathbf{in}\ M : \tau'} \quad \text{(T-Deref)}$$

$$\frac{\Gamma, x : \tau\ \mathit{ref}^{\kappa_1,\kappa_2} \vdash M : \tau' \qquad \kappa > 0}{\Gamma + V : \kappa_2\tau, x : \tau\ \mathit{ref}^{\kappa;\kappa_1,0} \vdash \mathbf{let}\ x :=^\kappa V\ \mathbf{in}\ M : \tau'} \quad \text{(T-Update)}$$

In the rule (T-Ref), $x : \lceil \tau \rceil\ \mathit{ref}^{\kappa_1,\kappa_2}$ means that the created reference cell may be read κ_2 times in M before the cell is updated and that each time the value is read, it is used as a value of type τ. So, the stored value V may be totally used as a value of type $\kappa_2\tau$. A tricky point about the rule (T-Update) is that the read count of x is 0 in the conclusion. This is because the currently stored value is replaced by V and therefore it is not read in $\mathbf{let}\ x :=^\kappa V\ \mathbf{in}\ M$ at all.

7 Preliminary Experiments

We have implemented a prototype type reconstruction system for the core-ML (i.e., SML [14] without modules) based on our quasi-linear type system and a simple profiler that executes the output program and counts the number of allocated heap values. We first describe the current status of the system in Section 7.1 and then report the results of simple experiments in Section 7.2. The prototype system will be available from `http://www.yl.is.s.u-tokyo.ac.jp/~koba/research/qlinear/`.

7.1 A prototype type reconstruction system

Following the extensions discussed in Section 6, we have implemented a prototype analyzer. It takes an expression of the core-ML as an input, performs type (and use) reconstruction and produces a use-annotated expression. It has been implemented by using the ML kit version 1 [4] as a front end, and supports full features of the core-ML: records, datatype declarations, references, and exceptions. Polymorphism on types and uses is based on the let-polymorphism discussed in Section 6.

Polymorphic recursion on uses would be sound (just as polymorphic recursion on regions is sound in the region inference [19]), but it is not supported currently. That is because the algorithm would become complex and also because the polymorphic recursion does not seem so crucial for our analysis.

The current system has the following limitations. It produces the least use annotation, not the best one (see Section 5); The analysis of the use of a reference cell is rough; Unnecessary uses are passed as parameters to use-polymorphic functions (they can be removed in the same manner as unnecessary region parameters are removed in a post-path of the region inference [5]); The current system is very slow for several known reasons (it is just because we preferred rapid prototyping and the system will be optimized in the future); A compiler that utilizes the analyzed information for in-place update, etc. has not been implemented yet.

7.2 Results of preliminary experiments

Table 1 shows the result of experiments. The columns 'zero,' 'linear,' and 'omega' respectively show how many heap values of use 0, 1, and ω are allocated dynamically in each program. The rightmost column shows what percentage of heap values are zero or linear. For a use-polymorphic function like $f : \forall i.(real^i \rightarrow^{\omega,\omega} real^i)$, the allocation was counted only once; in other words, creations of instances like $f[1]$ and $f[\omega]$ are not counted as the heap allocation (this is because the current analyzer infers not the use of each instance of a use-polymorphic function but the total use of all the instances: see Remark 6.2).

"sumlist10000" is a program that makes a list of integers from 0 to 10,000 and computes the sum of them. "qsort20" and "msort20" sort a list of 20 real numbers by using the quick sort and merge sort algorithms. They were written in a naive way; the main part of the quick sort program is:

```
fun quick ([]) = []
  | quick (x::l) =
        let val (l1,l2)=divide(x,l)
        in append(quick(l1), x::quick(l2)) end
```

"sieve2000" finds prime numbers less than 2,000 by using the sieve of Eratosthenes. "life" computes the first 10 generations of lives generated from the initial 44 lives. "dangle" and "reynolds3" are programs taken from [5] (with some parameters being changed). "reynolds3u" is a slightly modified version of "reynolds3," in which one function is uncurried so that our analysis works better.

In the cases of sumlist, merge/quick sorts and the sieve of Eratosthenes, almost all of the heap values are linear: non-linear values were only top-level functions. Moreover, by looking at the produced use-annotated expression, we can find that the cons cells generated in merge/quick sorts and the sieve of Eratosthenes can all be updated in-place.

In the case of the life (some curried functions in the original program were uncurried: see discussions in Section 9), dangle, and reynolds3, not all heap values are linear, but the number of linear

	zero	linear	omega	(zero+linear)/total
sumlist10000	0	40,001	2	100.0%
qsort20	0	448	4	99.1%
msort20	0	496	4	99.2%
sieve2000	0	256,455	8	100.0%
life	0	2,353,116	26,600	98.9%
Knuth-Bendix	0	10,339,410	2,949,292	77.8%
boyer	0	1,163,786	342,642	77.3%
mandelbrot	0	5,672,170	920,944	86.0%
dangle	20,000	20,032	34	99.9%
reynolds3	0	21,515	2,059	91.3%
reynolds3u	0	21,514	13	99.9%

Table 1: The number of allocated heap values

values is still huge enough to greatly reduce the need for garbage collection. In the Knuth-Bendix and boyer programs, the percentage of linear values is relatively smaller. This is probably because unification of first-order terms performed in the program causes sharing of many heap values.

One should, however, note that the percentages shown in the rightmost column do not necessarily indicate how much memory space can be saved by our analysis: compared with memory management using conventional garbage collection, extra memory space is required for representing use-polymorphic functions and its instances, and it is not yet clear how soon linear values can indeed be deallocated. Also, the current analysis is performed on unoptimized programs; other optimizations such as inlining and hoisting may reduce the ratio of linear values. Therefore, we know for sure the real impact of our analysis only after more serious experiments are carried out (for that purpose, some of the future work described in Section 9 must be completed).

8 Related Work

8.1 Previous linear type systems

To our knowledge, among previous linear type systems [3, 9, 21] that can automatically infer the usage of values, only Barendsen and Smetsers's uniqueness typing [3] takes an evaluation order into account. The effect of taking an evaluation order into account sometimes depends on a programming style, but it is evident at least for the following functions:

```
fun map f [] = []
```

```
  | map f (x::l) = f x::map f l
fun diff ([], S2) = []
  | diff (x::S1, S2) =
      if member(x, S2) then diff(S1, S2)
      else x::diff(S1,S2)
fun move (p, dx) = update(p, X, (#X p)+dx)
```

The function `f` in `map` and the list `S2` in `diff` (which is a function computing the set difference) are used many times, but are judged to be linear in the quasi-linear type system. The function `move` takes a record representing a point object as the first argument and adds `dx` to its `X` field. (Here, `update` is a primitive that takes a triple consisting of a record r, a label l, and a value v, and returns a record obtained by replacing the l field of r with v.) The point `p` is accessed twice, but it is also judged to be linear.

The uniqueness typing [3] is different from ours in many ways: the evaluation order is call-by-need,[4] their type system does not have "δ-type" of values that must be used up locally, and instead it relies on a separate analysis for analyzing the order of memory access (so, the analysis is not integrated as a use-type system, and it is rather complex).

Guzmán and Hudak [7] and Odersky [17] also proposed a kind of an extension of a linear type system, which can take an evaluation order into account and check that destructive operations on arrays or lists are safely used. Unlike ours, their approach is to let programmers explicitly declare where destructive operations should be performed (by using special primitives for destructive update of data structures) and check whether they are safe by performing type inference.

Another, rather technical novelty of our analysis is the definition of the operation "+." In the previous type system [8], $\tau_1 + \tau_2$ is defined only if τ_1 and τ_2 are identical except for their outermost uses. This restriction made the analysis inaccurate: for example, if a pair of real numbers is used as $real^1 \times^1 real^0$ in one place and as $real^0 \times^1 real^1$ in another place, both uses are coerced to $real^1 \times^1 real^1$ and the total use was counted as $real^\omega \times^\omega real^\omega$.

8.2 Region inference

There is an alternative approach to static memory management: region inference [5, 19]. The region inference abstracts a bunch of memory addresses as a region, and estimates its life-time by performing a kind of type inference. The region inference infers, in addition to the usual type information, which region each expression may access, and automatically inserts allocation and deallocation of regions.

Our type system and the region inference have both advantages and disadvantages. Because the life-time of data is estimated region-wise, it is difficult to use the region inference for in-place update

[4] Recently, they dealt also with strict let expressions, but the analysis for them seems to be more naive than our analysis [18].

(although it is possible in some cases by using multiplicity inference and storage mode analysis [5]). Another shortcoming of the region inference is that too many data are often merged into the same region (especially when recursive data structures, higher-order functions, and reference cells are used), and as a result, the analysis of the life-time of data sometimes becomes rough. (We do not intend to say that our analysis is always better for lists than the region inference. Indeed, if some cons cell of a list is accessed as an ω-value, our analysis assigns type τ *list*$^{\omega}$ to the list; hence no cons cells of the list can be deallocated automatically. In this case, the region inference would be much better.)

On the other hand, the advantages of the region inference are that it is completely independent of how often values are accessed, and that the deallocation of data in the same region can be performed in a constant time. So, it may be interesting to use our type system and the region inference as complementary methods for static memory management.

The goal of our analysis is also similar to that of the storage mode analysis [5], which was proposed as a complementary to the region inference. It analyzes whether each access to a value is the last access to the region of the value, and if so, it inserts a code to deallocate all values in the region. Thus, unlike our analysis, with the storage mode analysis, a value can be deallocated only after all the data in the region become garbage.

We give below examples for which both our analysis and the region inference work well, those for which our analysis works well but the region inference does not, and those for which the region inference works well but our analysis does not.

8.2.1 A program for which both our analysis and the region inference work well

Consider the following program `dangle` taken from [5]:

```
fun mklist 0 = []
  | mklist n = n::mklist(n-1);

fun cycle(m,f) =
    if m=0 then (m,f)
    else cycle(m-1, let val x=[(m,mklist 2000)]
                in fn ()=> #1(hd x)+f() end);

val r = cycle(100, fn()=>0);
```

In both the region inference and our analysis, the list generated by "`mklist 2000`" can be collected before `cycle` is called, although `x` is live at this moment and `x` has a pointer to the list. (In the case of our analysis, the list is not allocated in the first place, since the list creation is annotated with use 0.)

8.2.2 Programs for which our analysis works but the region inference does not

Consider the following program `reynolds3` taken from [5]:

```
datatype 'a tree = Lf | Br of 'a * 'a tree * 'a tree;

fun mk_tree 0 = Lf
  | mk_tree n = let val t=mk_tree(n-1) in Br(n,t,t) end;

fun member(x,[]) = false
  | member(x,x'::rest) = x=x' orelse member(x,rest);

fun search p Lf = false
  | search p (Br(x,t1,t2)) =
     if member(x,p) then true
     else search (x::p) t1 orelse search (x::p) t2;

val it = search [] (mk_tree 20)
```

In the region inference, the cons cell created by "`(x::p)`" can be deallocated only after "`search (x::p) t1 orelse search (x::p) t2`" is fully evaluated, while in our analysis, it can be deallocated after "`search (x::p) t1`" is evaluated.

Consider also the following function `merge`:

```
fun merge ([]:int list, l) = l
  | merge (l, []) = l
  | merge (x::l1, y::l2) = if x<y then x::merge(l1,y::l2)
                           else y::merge(x::l1,l2)
```

In the region inference, no cons cells of the lists $l1$ and $l2$ can be deallocated after `merge`$(l1, l2)$ is computed, because all cons cells are merged into the same region. On the other hand, unnecessary cons cells (cons cells matched to the patterns `x::l1` and `y::l2` in the above program) can be immediately deallocated in our analysis.

Consider another example:

```
let
  val r = ref (fn x=>x+1.0)
in
  ((!r)(2.0), !r)
end
```

In the region inference, 2.0 cannot be deallocated after the above expression is evaluated because it is stored in the region accessed by the function `fn x=>x+1.0`, which is still alive. On the other hand, in our analysis, 2.0 can be deallocated immediately after `(!r)(2.0)` is evaluated, because the type of `!r` is inferred as $real^1 \rightarrow^{\omega,\omega} real^\omega$.

Reasons why the region inference does not work In order to know why the region inference does not work for the above examples, one needs to know ideas of the region inference. In the region inference, a type is extended with information on where a value of the type is stored. For example, $(real, \rho)$ is the type of a real number that is stored in the region ρ. $((real, \rho_1) \rightarrow^{\{\rho_1,\rho_2\}} (real, \rho_2), \rho_3)$ is the type of a function that takes an argument stored in the region ρ_1, accesses the regions ρ_1 and ρ_2, and returns a real number stored in the region ρ_2. The function itself is stored in the region ρ_3. By performing type inference based on such a type system, operations for allocating/deallocating regions can be inserted. For example, if a closed expression e is inferred to have a type $(real, \rho_1)$ and a value is allocated in the region ρ_2 inside e, we know that the value is not alive and can be deallocated after e has been evaluated.

The main reason why the region inference does not work for the first and second example is that all the cons cells of a list must be stored in the same region. Because we must represent each type by using a finite expression, it is impossible to distinguish the region of each cell that constitutes a recursive data structure. So, for example, the type of a list of real numbers must be something like $((real, \rho_1)\ list, \rho_2)$, where ρ_1 is the region in which the elements of the list are stored, and ρ_2 is the region in which the cons cells are stored. Thus, cons cells and elements that are once put into the same list can be deallocated only after all of them become garbage.

The reason for the third example is that without region polymorphism [19], region-annotated types can express only poor dataflow information. A region-polymorphic type:

$$\forall \rho_1, \rho_2.((real, \rho_1) \rightarrow^{\{\rho_1,\rho_2\}} (real, \rho_2), \rho_3)$$

means that a function of that type takes its argument stored in some region ρ_1 and returns a result stored in another region ρ_2; so, it subsumes information represented by a use-annotated type $real^\delta \rightarrow^{\omega,\omega} real^\omega$ in our type system. However, in the third example, `!r` can be assigned only a monomorphic type: $((real, \rho_1) \rightarrow^{\{\rho_1,\rho_2\}} (real, \rho_2), \rho_3)$. So, if `!r` is used in another place (and indeed this may be the case because `!r` escapes), the argument must be stored in the same region ρ_1, which means that the region ρ_1 can be deallocated only after it becomes certain that there is no more call to the function `!r`.

8.2.3 A program for which the region inference works well but our analysis does not

Consider the following program

```
fun f (x:real) = fn y=> x+y
val it = let val g = f(1.0) in g(2.0)+g(3.0) end
```

In our analysis, the use of `1.0` is judged to be ω and cannot be deallocated (because upon each invocation, `g` uses `x` as a value of use of at least 1, and `g` is called twice). On the other hand, the region inference can deallocate `1.0` after the whole expression is evaluated.

Consider also the following program:

```
fun choose(b, x, y) = if b then x else y
val it = let val z=1.0 in choose(true, z, z)+2.0 end
```

1.0 is inferred to be an ω-value and cannot be deallocated in our analysis, while it can be deallocated in the region inference.

The reason why our analysis does not work for the first example is that the dataflow information represented by the use δ is too naive. The second example reveals a limitation of our analysis in counting value access: without knowing the value of `b`, our analysis can only find that both `x` and `y` may be used at most once (if the result is used once), and therefore, it infers that `z` may be used twice.

9 Conclusion and Future Work

We proposed an extended linear type system that can elegantly take an evaluation order into account, and proved its correctness. Static memory management like the one proposed here and the region inference is currently less popular than conventional garbage collection. However, we think it will become very important in the near future. First, static memory management is especially attractive in parallel/distributed environments, since it requires much less communications/synchronizations than conventional garbage collection. Second, with the increasing importance of cache memory, saving the memory space for a program is also likely to save its execution time.

The type system proposed in this paper is for call-by-value languages; it is not yet clear whether a similar type system can be developed for lazy functional languages.

Much work is left to be done to apply our type system to a compiler of ML and know its real impact. We need to work at least on the following issues (although they seem to be fairly straightforward except for the last issue):

Refinement of the type inference system As discussed in Section 5.2, the least use annotation may not be *optimal* from the viewpoint of memory management; so, we need to modify the analyzer so that it can produce a better use annotation.

Reduction of the cost for use passing Since passing uses to use-polymorphic functions takes some extra cost, we need to reduce it by dropping unnecessary uses (just as unnecessary region parameters in region inference [5]) and by using a similar technique to type lifting [20].

Transformation for in-place updates We need to implement a compilation path that finds places where deallocation of a heap value is immediately followed by allocation of another value of the same type and replaces it with in-place update.

Combination with conventional garbage collection Since the linear-type-based memory management can automatically deallocate only quasi-linear values, we need a conventional garbage collector as well. There is, however, a subtle problem: since the linear-type-based memory management is not based on the pointer traversal information, it may create a dangling pointer (just as the region-based memory managements does [19]). For example, when the closure $(\lambda x.(\mathbf{fst}(y) + x), \{y = \langle 1.0, 2.0\rangle\})$ is traced at garbage collection time, the second element 2.0 of y may have already been deallocated. There are two ways for dealing with this problem. One way is to exclude the use 0 from the type system so that dangling pointers cannot be created. The other way, which we are currently exploring (with Atsushi Igarashi), is to use the idea of tag-free garbage collection [15, 20]: we can utilize use-annotated types for tracing heap values at garbage collection time, instead of conventional types. For example, from the type $\mathit{real}^1 \times^\omega \mathit{real}^0$ of y in the above closure, it is known that the second element of y will not be accessed by the closure and hence it need not be traced by a garbage collector.

The following improvement of the accuracy of the analysis is also future work.

Taking the order of access to different variables into account Because the type system cannot deal with the order of access to different variables, the analysis can be rough when variables are aliased. For example, consider an expression $\mathbf{let}\ y = x\ \mathbf{in}\ \mathbf{fst}^\delta(x) + \mathbf{fst}^1(y)$. Since x and y refer to the same heap value, we could regard x as a linear value; however, the current type system judges x to be an ω-value. We can overcome this problem by representing a type environment as a poset of type bindings in order to express the order of access to different variables, as in an earlier version [10] of Kobayashi's type system for deadlock-freedom [11].

Combining our analysis with other analyses Our analysis of δ-values is weak in dealing with curried functions. Consider an expression $(\lambda z.(\mathbf{fst}(z) + 1.0))\langle 2.0, 3.0\rangle$ and its curried version $((\lambda x.\lambda y.(x + 1.0))2.0)3.0$. For the former expression, δ can be assigned to 2.0, while 1 must be assigned to it for the latter one. This problem may not be so serious because the ordinary compiler optimization uncurries functions as far as possible, but it may be interesting to improve the analysis by using more accurate dataflow information like the one obtained by the region inference.

Acknowledgment

We would like to thank Atsushi Igarashi, Martin Odersky, Kenjiro Taura, Mads Tofte, and the anonymous referees for useful discussions and comments.

References

[1] Henry G. Baker. Lively linear lisp – look ma, no garbage! *ACM Sigplan Notices*, 27(8):89–98, 1992.

[2] Henry G. Baker. A linear logic quicksort. *ACM Sigplan Notices*, 29(2):13–18, 1994.

[3] Erik Barendsen and Sjaak Smetsers. Conventional and uniqueness typing in graph rewrite systems. Technical Report CSI-R9328, Computer Science Institute, University of Nijmegen, 1993. An extended abstract appeared in Proc. of FST&TCS 12, Springer LNCS 761, pp.41-51.

[4] Lars Birkedal, Nick Rothwell, Mads Tofte, and David N. Turner. The ML Kit (Version 1). Technical Report 93/14, Department of Computer Science, University of Copenhagen, 1993.

[5] Lars Birkedal, Mads Tofte, and Magnus Vejlstrup. From region inference to von neumann machines via region representation inference. In *Proceedings of ACM SIGPLAN/SIGACT Symposium on Principles of Programming Languages*, pages 171–183, 1996.

[6] Jean-Yves Girard. Linear logic. *Theoretical Computer Science*, 50:1–102, 1987.

[7] Juan G. Guzmán and Paul Hudak. Single-threaded polymorphic lambda calculus. In *Proceedings of IEEE Symposium on Logic in Computer Science*, pages 333–343, 1990.

[8] Atsushi Igarashi. Type-based analysis of usage of values for concurrent programming languages. Master's thesis, Department of Information Science, University of Tokyo, 1997.

[9] Atsushi Igarashi and Naoki Kobayashi. Type-based analysis of usage of communication channels for concurrent programming languages. In *Proceedings of International Static Analysis Symposium (SAS'97)*, volume 1302 of *Lecture Notes in Computer Science*, pages 187–201. Springer-Verlag, 1997.

[10] Naoki Kobayashi. A Partially Deadlock-free Typed Process Calculus (I) – A Simple System –. Technical Report 96-02, Department of Information Science, University of Tokyo, September 1996.

[11] Naoki Kobayashi. A partially deadlock-free typed process calculus. *ACM Transactions on Programming Languages and Systems*, 20(2):436–482, 1998. A preliminary summary appeared in Proceedings of LICS'97, pages 128–139.

[12] Naoki Kobayashi, Benjamin C. Pierce, and David N. Turner. Linearity and the pi-calculus. In *Proceedings of ACM SIGPLAN/SIGACT Symposium on Principles of Programming Languages*, pages 358–371, January 1996.

[13] Ian Mackie. Lilac : A functional programming language based on linear logic. *Journal of Functional Programming*, 4(4):1–39, October 1994.

[14] Robin Milner, Mads Tofte, Robert Harper, and David MacQueen. *The Definition of Standard ML (Revised)*. The MIT Press, 1997.

[15] Greg Morrisett. *Compiling with Types*. PhD thesis, School of Computer Science, Carnegie Mellon University, 1995.

[16] Greg Morrisett, Matthias Felleisen, and Robert Harper. Abstract models of memory management. In *Proceedings of Functional Programming Languages and Computer Architecture*, pages 66–76, 1995.

[17] Martin Odersky. Observers for linear types. In *Proceedings of 4th European Symposium on Programming (ESOP'92)*, volume 582 of *Lecture Notes in Computer Science*, pages 390–407. Springer-Verlag, 1992.

[18] Rinus Plasmeijer and Marko van Eekelen. Concurrent Clean ver.1.3 language report. available from `http://www.cs.kun.nl/~clean/`, 1997.

[19] Mads Tofte and Jean-Pierre Talpin. Implementing the call-by-value lambda-calculus using a stack of regions. In *Proceedings of ACM SIGPLAN/SIGACT Symposium on Principles of Programming Languages*, pages 188–201, 1994.

[20] Andrew Tolmach. Tag-free garbage collection using explicit type parameters. In *Proceedings of ACM Conference on Lisp and Functional Programming*, pages 1–11, 1994.

[21] David N. Turner, Philip Wadler, and Christian Mossin. Once upon a type. In *Functional Programming Languages and Computer Architecture*, San Diego, California, 1995.

A Proofs

A.1 Laws on operations on uses, types, and type environments

We first list several laws on operations defined in Section 3. They are used frequently in the proofs below.

Lemma A.1:

1. The operation $+$ (on uses, types, and type environments) is associative and commutative.
2. The operation $;$ (on uses, types, and type environments) is associative.
3. The operation $\cdot$ on uses is associative and commutative.
4. The unary operations $\lceil _ \rceil$ and $\lfloor _ \rfloor$ are monotonic.
5. $\kappa_1 + \kappa_2 \geq \kappa_1; \kappa_2$, $\tau_1 + \tau_2 \geq \tau_1; \tau_2$, and $\Gamma_1 + \Gamma_2 \geq \Gamma_1; \Gamma_2$.
6. $(\kappa_1 + \kappa_2) - \kappa_3 \geq (\kappa_1 - \kappa_3) + \kappa_2$, $(\tau_1 + \tau_2) - \tau_3 \geq (\tau_1 - \tau_3) + \tau_2$, and $(\Gamma_1 + \Gamma_2) - \Gamma_3 \geq (\Gamma_1 - \Gamma_3) + \Gamma_2$.
7. $(\kappa_1; \kappa_2) - \kappa_1 \geq \kappa_2$, $(\tau_1; \tau_2) - \tau_1 \geq \tau_2$, and $(\Gamma_1; \Gamma_2) - \Gamma_1 \geq \Gamma_2$.
8. $(\kappa_1; \kappa_2) \cdot \kappa_3 = (\kappa_1 \cdot \kappa_3); (\kappa_2 \cdot \kappa_3)$, $(\kappa_1; \kappa_2) \cdot \tau = (\kappa_1 \cdot \tau); (\kappa_2 \cdot \tau)$, and $(\kappa_1; \kappa_2) \cdot \Gamma = (\kappa_1 \cdot \Gamma); (\kappa_2 \cdot \Gamma)$
9. $\lceil \kappa_1 \rceil + \kappa_2 = \lceil \kappa_1 \rceil; \kappa_2$, $\lceil \tau_1 \rceil + \tau_2 = \lceil \tau_1 \rceil; \tau_2$, and $\lceil \Gamma_1 \rceil + \Gamma_2 = \lceil \Gamma_1 \rceil; \Gamma_2$.
10. $(\kappa_1 + \kappa_2); (\kappa_3 + \kappa_4) \leq (\kappa_1; \kappa_3) + (\kappa_2; \kappa_4)$, $(\tau_1 + \tau_2); (\tau_3 + \tau_4) \leq (\tau_1; \tau_3) + (\tau_2; \tau_4)$, and $(\Gamma_1 + \Gamma_2); (\Gamma_3 + \Gamma_4) \leq (\Gamma_1; \Gamma_3) + (\Gamma_2; \Gamma_4)$.

Proof: Trivial from the definitions of the operations. □

A.2 Proof of Theorem 4.9

Definition A.2 [outermost use]: The *outermost use* of a type τ, written $Use(\tau)$, is defined by: $Use(\tau_1 \times^{\kappa} \tau_2) = \kappa$ and $Use(\tau_1 \rightarrow^{\kappa_1, \kappa_2} \tau_2) = \kappa_1$. $Use(int)$ is undefined.

Lemma A.3: If $\Gamma \vdash D : \tau$ and $D \xrightarrow{x=h^{\kappa}} D'$, then $Use(\Gamma(x)) \geq \kappa$.

Proof: Trivial induction on the derivation of $D \xrightarrow{x=h^{\kappa}} D'$. □

Proof of Theorem 4.9: Suppose $\Gamma \vdash D : \tau$ and $D \xrightarrow{\epsilon} \mathbf{Error}$. Then, D has a subterm of the form $\mathbf{letrec}\ x = h^{\kappa}\ \mathbf{in}\ D'$ such that $\Gamma' \vdash \mathbf{letrec}\ x = h^{\kappa}\ \mathbf{in}\ D' : \tau'$, $D' \xrightarrow{x=h^{\kappa'}} D''$, and $(\kappa' > \kappa) \vee (\kappa' = 0)$. By typing rules for dynamic expressions, $\kappa' \neq 0$ and there must be Γ'' such that $\Gamma'', x : \tau'' \vdash D' : \tau'$ and $\kappa \geq \mathit{Use}(\tau'')$. By Lemma A.3, it must be that $\kappa \geq \mathit{Use}(\tau'') \geq \kappa'$, which contradicts with $\kappa' > \kappa$. □

A.3 Proof of Theorem 4.10

We will show the theorem by induction on the derivation of $D \longrightarrow D'$. Before proving the theorem, we need several lemmas. The first lemma says that we can obtain syntax-directed typing rules by eliminating (T-Weak).

Lemma A.4 [Elimination of weakening]: If $\Gamma \vdash D : \tau$ is derivable, then it is derivable also by using (T-Weak) only after the rule (T-Var).

Proof: This follows from the fact that (T-Weak) applied below rules except for (T-Var) can be permuted upwards. □

Lemma A.5 [Renaming]: If $\Gamma, x : \tau_1 \vdash D : \tau_2$ and $\Gamma + V : \tau_1$ is well defined, then $\Gamma + V : \tau_1 \vdash [V/x]D : \tau_2$.

Proof: Trivial induction on the derivation of $\Gamma, x : \tau_1 \vdash D : \tau_2$. □

The following two lemmas show how typing is changed by reductions labeled with $x = h^{\kappa}$.

Lemma A.6: If $\Gamma, x : \tau_1 \times^{\kappa} \tau_2 \vdash D : \tau_3$ and $D \xrightarrow{x=\langle V_1, V_2 \rangle^{\kappa'}} D'$, then $\tau_1 = \tau_1' + \tau_1''$, $\tau_2 = \tau_2' + \tau_2''$, and $\Gamma + V_1 : \tau_1' + V_2 : \tau_2', x : \tau_1'' \times^{\kappa - \kappa'} \tau_2'' \vdash D' : \tau_3$ for some $\tau_1', \tau_1'', \tau_2', \tau_2''$.

Proof: We show the lemma by induction on the derivation of $D \xrightarrow{x=\langle V_1, V_2 \rangle^{\kappa'}} D'$, with case analysis on the last rule.

- Case for (DR-Fst):
  In this case, $D = \mathbf{let}\ u = \mathbf{fst}^{\kappa'}(x)\ \mathbf{in}\ D_1$ and $D' = [V_1/u]D_1$. Suppose (1)$\Gamma, x : \tau_1 \times^{\kappa} \tau_2 \vdash D : \tau_3$. By the rule (T-Fst), we have

  (2)$\Gamma, u : \tau_1', x : \tau_1'' \times^{\kappa''} \tau_2'' \vdash D_1 : \tau_3$
  (3)$\tau_1 = \tau_1' + \tau_1''$
  (4)$\tau_2 = \tau_2'' = \mathit{null}(\tau_2'') + \tau_2''$
  (5)$\kappa = \kappa'; \kappa''$

By applying Lemma A.5 to (2), we obtain (6) $\Gamma + V_1 : \tau_1', x : \tau_1'' \times^{\kappa''} \tau_2'' \vdash [V_1/u]D_1 : \tau_3$. By the fact $\kappa - \kappa' \geq \kappa''$ (which follows from (5)) and the rule (T-Weak), we have $\Gamma + V_1 : \tau_1' + V_2 : null(\tau_2''), x : \tau_1'' \times^{\kappa - \kappa'} \tau_2'' \vdash [V_1/u]D_1 : \tau_3$.

- Case for (DR-Snd): Similar to the case for (DR-Fst)
- Case for (DR-ConRec):

  In this case, (1)$D = \textbf{letrec}\ w = h^{\kappa_1}\ \textbf{in}\ D_1$, (2)$D' = \textbf{letrec}\ w = h^{\kappa_1}\ \textbf{in}\ D_1'$, and (3)$D_1 \xrightarrow{x=\langle V_1, V_2\rangle^{\kappa'}} D_1'$. Suppose (4)$\Gamma, x : \tau_1 \times^{\kappa} \tau_2 \vdash D : \tau_3$.

  By (DT-Heap),

  (5)$\Gamma_1, x : \tau_3 \times^{\kappa_2} \tau_4 \vdash w = h^{\kappa_1} : \tau_7$
  (6)$\Gamma_2, x : \tau_5 \times^{\kappa_3} \tau_6, w : \tau_7 \vdash D_1 : \tau$
  (7)$\Gamma = \Gamma_1 + \Gamma_2$
  (8)$(\tau_3 \times^{\kappa_2} \tau_4) + (\tau_5 \times^{\kappa_3} \tau_6) = \tau_1 \times^{\kappa} \tau_2$

  for some $\Gamma_1, \Gamma_2, \tau_3, \tau_4, \tau_5, \tau_6, \tau_7, \kappa_2, \kappa_3$. By (3), (6), and induction hypothesis,

  (9)$\Gamma_2 + V_1 : \tau_5' + V_2 : \tau_6', x : \tau_5'' \times^{\kappa_3 - \kappa'} \tau_6'', w : \tau_7 \vdash D_1' : \tau$
  (10)$\tau_5' + \tau_5'' = \tau_5$
  (11)$\tau_6' + \tau_6'' = \tau_6$

  for some $\tau_5', \tau_5'', \tau_6', \tau_6''$. By (5), (9) and (DT-Heap),

  (12)$\Gamma_1 + \Gamma_2 + V_1 : \tau_5' + V_2 : \tau_6', x : (\tau_3 + \tau_5'') \times^{\kappa_2 + (\kappa_3 - \kappa')} (\tau_4 + \tau_6'') \vdash D' : \tau$.

  Let $\tau_1' = \tau_5', \tau_2' = \tau_6', \tau_1'' = \tau_3 + \tau_5''$, and $\tau_2'' = \tau_4 + \tau_6''$. Then, by (7), (9), (10), and (11), we have $\tau_1' + \tau_1'' = \tau_1$, $\tau_2' + \tau_2'' = \tau_2$, and $\Gamma + V_1 : \tau_1' + V_2 : \tau_2', x : \tau_1'' \times^{\kappa_2 + (\kappa_3 - \kappa')} \tau_2'' \vdash D' : \tau$. Since $\kappa - \kappa' = (\kappa_2 + \kappa_3) - \kappa' \geq \kappa_2 + (\kappa_3 - \kappa')$, by using (T-Weak), we obtain $\Gamma + V_1 : \tau_1' + V_2 : \tau_2', x : \tau_1'' \times^{\kappa - \kappa'} \tau_2'' \vdash D' : \tau$ as required.

□

Lemma A.7: If $\Gamma, x : \tau_1 \rightarrow^{\kappa_1, \kappa_2} \tau_2 \vdash D : \tau$ and $D \xrightarrow{x=\lambda^{\kappa'} y.M_1} D'$, then $\Gamma + \Gamma_1,\ x : \tau_1 \rightarrow^{(\kappa_1 + \kappa_3) - \kappa', (\kappa_2 + \kappa_4) - 1} \tau_2 \vdash D' : \tau$ holds for any Γ_1 such that $\Gamma_1, x : \tau_1 \rightarrow^{\kappa_3, \kappa_4} \tau_2, y : \tau_1 \vdash M_1 : \tau_2$ and $\Gamma + \Gamma_1$ is well defined.

Proof: Induction on the derivation of $D \xrightarrow{x=\lambda^{\kappa'} y.M_1} D'$, with case analysis on the last rule.

- Case for (DR-App):
  In this case, (1)$D = \mathbf{let}\ u = \mathit{apply}^{\kappa'}(x, V)\ \mathbf{in}\ D_2$, and (2)$D' = \mathbf{let}\ u = [V/y]M_1\ \mathbf{in}\ D_2$. Suppose (3)$\Gamma, x : \tau_1 \to^{\kappa_1,\kappa_2} \tau_2 \vdash D : \tau$ and (4)$\Gamma_1, y : \tau_1, x : \tau_1 \to^{\kappa_3,\kappa_4} \tau_2 \vdash M_1 : \tau_2$. By (3), we have

  (5)$\Gamma_2, x : \tau_1 \to^{\kappa_1',\kappa_2'} \tau_2, u : \tau_2 \vdash D_2 : \tau$
  (6)$\kappa_1 = \kappa'; \kappa_1'$
  (7)$\kappa_2 = 1; \kappa_2'$
  (8)$\Gamma = (V : \tau_1); \Gamma_2$

  for some $\Gamma_2, \kappa_1', \kappa_2'$. By applying Lemma A.5 to (4), we have

  (9)$\Gamma_1 + V : \tau_1, x : \tau_1 \to^{\kappa_3,\kappa_4} \tau_2 \vdash [V/y]M_1 : \tau_2$.

  By applying (T-Let) to (5) and (9), we obtain

  (10)$(\Gamma_1 + V : \tau_1, x : \tau_1 \to^{\kappa_3,\kappa_4} \tau_2); (\Gamma_2, x : \tau_1 \to^{\kappa_1',\kappa_2'} \tau_2) \vdash D' : \tau$.

  Here, we have $\kappa_3; \kappa_1' \le \kappa_1 + \kappa_3 - \kappa'$ by the following inequalities:

  $$\begin{array}{rcl} (\kappa_1 + \kappa_3) - \kappa' & = & ((\kappa'; \kappa_1') + \kappa_3) - \kappa' \\ & \ge & (\kappa'; \kappa_1') - \kappa' + \kappa_3 \\ & \ge & \kappa_1' + \kappa_3 \\ & \ge & \kappa_3; \kappa_1' \end{array}$$

  (Here, we used the fact $(\kappa_1; \kappa_2) - \kappa_1 \ge \kappa_2$.) Similarly, $\kappa_4; \kappa_2' \le \kappa_2 + \kappa_4 - 1$. So,

  $$\begin{array}{rl} & (\Gamma_1 + V : \tau_1, x : \tau_1 \to^{\kappa_3,\kappa_4} \tau_2); (\Gamma_2, x : \tau_1 \to^{\kappa_1',\kappa_2'} \tau_2) \\ = & ((\Gamma_1 + V : \tau_1); \Gamma_2), x : \tau_1 \to^{\kappa_3;\kappa_1',\kappa_4;\kappa_2'} \tau_2 \\ \le & \Gamma_1 + (V : \tau_1; \Gamma_2), x : \tau_1 \to^{\kappa_1+\kappa_3-\kappa',\kappa_2+\kappa_4-1} \tau_2 \\ = & \Gamma_1 + \Gamma, x : \tau_1 \to^{\kappa_1+\kappa_3-\kappa',\kappa_2+\kappa_4-1} \tau_2 \end{array}$$

  By applying (T-Weak) to (10), we obtain

  $\Gamma_1 + \Gamma, x : \tau_1 \to^{\kappa_1+\kappa_3-\kappa',\kappa_2+\kappa_4-1} \tau_2 \vdash D' : \tau$

  as required.

- Case for (DR-ConRec): In this case, (1)$D = \mathbf{letrec}\ w = h^{\kappa_5}\ \mathbf{in}\ D_2$, (2)$D' = \mathbf{letrec}\ w = h^{\kappa_5}\ \mathbf{in}\ D_2'$, and (3)$D_2 \xrightarrow{x=\lambda^{\kappa'} y.M_1} D_2'$. Suppose (4)$\Gamma, x : \tau_1 \to^{\kappa_1,\kappa_2} \tau_2 \vdash D : \tau$ and

(5)$\Gamma_1, x:\tau_1 \rightarrow^{\kappa_3,\kappa_4} \tau_2, y:\tau_1 \vdash M_1 : \tau_2$. We need to show $\Gamma + \Gamma_1, x:\tau_1 \rightarrow^{\kappa_1+\kappa_3-\kappa', \kappa_2+\kappa_4-1} \tau_2 \vdash D' : \tau$. By (DT-HEAP) and (4), it must be that

$$(6)\Gamma_2, x:\tau_1 \rightarrow^{\kappa_6,\kappa_7} \tau_2 \vdash w = h^{\kappa_5} : \tau_3$$
$$(7)\Gamma_3, x:\tau_1 \rightarrow^{\kappa_8,\kappa_9} \tau_2, w:\tau_3 \vdash D_2 : \tau$$
$$(8)\Gamma = \Gamma_2 + \Gamma_3$$
$$(9)\kappa_1 = \kappa_6 + \kappa_8$$
$$(10)\kappa_2 = \kappa_7 + \kappa_9$$

for some $\Gamma_2, \Gamma_3, \kappa_4, \kappa_5, \kappa_6, \kappa_7, \kappa_8, \kappa_9$. By (3), (6) and induction hypothesis, $\Gamma_3 + \Gamma_1, w:\tau_3, x:\tau_1 \rightarrow^{\kappa_8+\kappa_3-\kappa', \kappa_9+\kappa_4-1} \tau_2 \vdash D_2' : \tau$. By using (DT-HEAP), we obtain

$$\Gamma_2 + \Gamma_3 + \Gamma_1, x:\tau_1 \rightarrow^{\kappa_6+(\kappa_8+\kappa_3-\kappa'), \kappa_7+(\kappa_9+\kappa_4-1)} \tau_2 \vdash D' : \tau.$$

Since $\kappa_6 + (\kappa_8 + \kappa_3 - \kappa') \leq (\kappa_6 + \kappa_8 + \kappa_3) - \kappa' = \kappa_1 + \kappa_3 - \kappa'$ and $\kappa_7 + (\kappa_9 + \kappa_4 - 1) \leq \kappa_2 + \kappa_4 - 1$, by using (T-WEAK) we obtain

$$\Gamma + \Gamma_1, x:\tau_1 \rightarrow^{\kappa_1+\kappa_3-\kappa', \kappa_2+\kappa_4-1} \tau_2 \vdash D' : \tau$$

as required.

□

Next, we shall show that the reduction (DR-VAR) preserves typing (Lemma A.11 below). We need the three technical lemmas (Lemma A.8, A.9, and A.10) below.

Lemma A.8: If $\Gamma_1 \vdash x = h^{\kappa_1} : \tau_1$ and $\Gamma_2 \vdash x = h^{\kappa_2} : \tau_2$, and if both $\Gamma_1 + \Gamma_2$ and $\tau_1 + \tau_2$ are well defined, then $\Gamma_1 + \Gamma_2 \vdash x = h^{\kappa_1+\kappa_2} : \tau_1 + \tau_2$.

Proof: Trivial from the rules (DT-PAIR) and (DT-ABS). □

Lemma A.9: If $\Gamma \vdash y = h^{\kappa} : \tau$ then $\Gamma' \vdash y = h^{\lfloor\kappa\rfloor} : \lfloor\tau\rfloor$ and $\Gamma' \leq \lfloor\Gamma\rfloor$ for some Γ'.

Proof: We show this by case analysis on h.

- Case where h is of the form $\langle V_1, V_2\rangle$.
  It must be that $\Gamma = V_1 : \tau_1 + V_2 : \tau_2$ and $\tau = \tau_1 \times^{\kappa} \tau_2$ for some τ_1 and τ_2. By (DT-PAIR), we have $V_1 : \lfloor\tau_1\rfloor + V_2 : \lfloor\tau_2\rfloor \vdash y = h^{\lfloor\kappa\rfloor} : \lfloor\tau_1\rfloor \times^{\lfloor\kappa\rfloor} \lfloor\tau_2\rfloor$. Let $\Gamma' = V_1 : \lfloor\tau_1\rfloor + V_2 : \lfloor\tau_2\rfloor$. Then $\Gamma' \vdash y = h^{\lfloor\kappa\rfloor} : \lfloor\tau\rfloor$ and $\Gamma' \leq \lfloor\Gamma\rfloor$ as required.

- Case where h is of the form $\lambda x.M$.
  It must be that
  $$\Gamma_1, x : \tau_1, y : \tau_1 \rightarrow^{\kappa_1,\kappa_2} \tau_2 \vdash M : \tau_2$$
  $$\tau = \tau_1 \rightarrow^{\kappa_3,\kappa_4} \tau_2$$
  $$\kappa \geq \kappa_3(1+\kappa_1)$$
  $$\Gamma = \kappa_4(1+\kappa_2)\lceil\Gamma_1\rceil$$
  for some $\Gamma_1, \tau_1, \tau_2, \kappa_1, \kappa_2, \kappa_3, \kappa_4$. By (DT-Abs), we have $\lfloor\kappa_4\rfloor(1+\kappa_2)\lceil\Gamma_1\rceil \vdash y = h^{\lfloor\kappa_3\rfloor(1+\kappa_1)} : \tau_1 \rightarrow^{\lfloor\kappa_3\rfloor,\lfloor\kappa_4\rfloor} \tau_2$. Since $\lfloor\kappa_4\rfloor(1+\kappa_2)\lceil\Gamma_1\rceil = \lfloor\kappa_4\rfloor\lfloor 1+\kappa_2\rfloor\lceil\Gamma_1\rceil = \lfloor\Gamma\rfloor$ and $\lfloor\kappa_3\rfloor(1+\kappa_1) = \lfloor\kappa_3(1+\kappa_1)\rfloor \leq \lfloor\kappa\rfloor$, we have $\lfloor\Gamma\rfloor \vdash y = h^{\lfloor\kappa\rfloor} : \lfloor\tau\rfloor$ as required.

□

Lemma A.10: If $\Gamma \vdash$ **letrec** $\vec{y} = \vec{h}^{\vec{\kappa}}$ **in** $V : \lceil\tau\rceil$, then $\lfloor\Gamma\rfloor \vdash$ **letrec** $\vec{y} = \vec{h}^{\lfloor\vec{\kappa}\rfloor}$ **in** $V : \lceil\tau\rceil$.

Proof: Induction on the length of $\vec{y}$.

- Base case:
  Suppose $\Gamma \vdash V : \lceil\tau\rceil$. Since it must be derived by (T-Var) and (T-Weak), it must be that $\Gamma \geq V : \lceil\tau\rceil$. Since $\lfloor\Gamma\rfloor \geq V : \lceil\tau\rceil$, we have $\lfloor\Gamma\rfloor \vdash V : \lceil\tau\rceil$.

- Induction step: Suppose $\Gamma \vdash$ **letrec** $y' = h'^{\kappa'}, \vec{y} = \vec{h}^{\vec{k}}$ **in** $V : \lceil\tau\rceil$. By (DT-Heap), it must be that
  $$\Gamma_1 \vdash y' = h'^{\kappa'} : \tau_1$$
  $$\Gamma_2, y' : \tau_1 \vdash \textbf{letrec } \vec{y} = \vec{h}^{\vec{k}} \textbf{ in } V : \lceil\tau\rceil$$
  $$\Gamma = \Gamma_1 + \Gamma_2.$$
  By Lemma A.9 and induction hypothesis, we have
  $$\Gamma_1' \vdash y' = h'^{\lfloor\kappa'\rfloor} : \lfloor\tau_1\rfloor$$
  $$\lfloor\Gamma_2\rfloor, y' : \lfloor\tau_1\rfloor \vdash \textbf{letrec } \vec{y} = \vec{h}^{\lfloor\vec{k}\rfloor} \textbf{ in } V : \lceil\tau\rceil$$
  $$\Gamma_1' \leq \lfloor\Gamma_1\rfloor$$
  By using (DT-Heap) and the fact that $\lfloor\Gamma\rfloor = \lfloor\Gamma_1 + \Gamma_2\rfloor \geq \lfloor\Gamma_1\rfloor + \lfloor\Gamma_2\rfloor \geq \Gamma_1' + \lfloor\Gamma_2\rfloor$, we have $\lfloor\Gamma\rfloor \vdash$ **letrec** $y' = h'^{\lfloor\kappa'\rfloor}, \vec{y} = \vec{h}^{\lfloor\vec{k}\rfloor}$ **in** $V : \lceil\tau\rceil$ as required.

□

Lemma A.11: If $\Gamma \vdash$ **let** $x =$ (**letrec** $\vec{z} = \vec{h}^{\vec{\kappa_1}}, \vec{w} = \vec{h'}^{\vec{\kappa_3}}$ **in** V) **in** (**letrec** $\vec{z} = \vec{h}^{\vec{\kappa_2}}$ **in** M) $: \tau$, then $\Gamma \vdash$ **letrec** $\vec{z} = \vec{h}^{\lfloor\vec{\kappa_1}\rfloor;\vec{\kappa_2}}, \vec{w} = \vec{h'}^{\lfloor\vec{\kappa_3}\rfloor}$ **in** $[V/x]M : \tau$.

Proof: It is sufficient to show the case where $\vec{w}$ is an empty sequence, because $\Gamma \vdash \textbf{let } x = (\textbf{letrec } \vec{z} = \vec{h}^{\vec{\kappa_1}}, \vec{w} = \vec{h'}^{\vec{\kappa_3}} \textbf{ in } V) \textbf{ in } (\textbf{letrec } \vec{z} = \vec{h}^{\vec{\kappa_2}} \textbf{ in } M) : \tau$ implies $\Gamma \vdash \textbf{let } x = (\textbf{letrec } \vec{z} = \vec{h}^{\vec{\kappa_1}}, \vec{w} = \vec{h'}^{\vec{\kappa_3}} \textbf{ in } V) \textbf{ in } (\textbf{letrec } \vec{z} = \vec{h}^{\vec{\kappa_2}}, \vec{w} = \vec{h'}^{\vec{0}} \textbf{ in } M) : \tau$ (by the rules (DT-Pair) and (DT-Abs)). We show by induction on the length of the sequence $\vec{z}$.

- Base case: Suppose $\Gamma \vdash \textbf{let } x = V \textbf{ in } M : \tau$. Then, $(1)\Gamma_1 \vdash V : \lceil \tau_1 \rceil$, $(2)\Gamma_2, x : \lceil \tau_1 \rceil \vdash M : \tau$, $(3)\Gamma = \Gamma_1; \Gamma_2$ and $(4)\Gamma_1 \geq V : \lceil \tau_1 \rceil$. By applying Lemma A.5 to (2), we obtain $\Gamma_2 + V : \lceil \tau_1 \rceil \vdash [V/x]M : \tau$. Since $\Gamma = \Gamma_1; \Gamma_2 \geq (V : \lceil \tau_1 \rceil); \Gamma_2 = \Gamma_2 + V : \lceil \tau_1 \rceil$, we have $\Gamma \vdash [V/x]M : \tau$ by (T-Weak).

- Induction step: Suppose

$$\Gamma \vdash \textbf{let } x = (\textbf{letrec } z = h^{\kappa}, \vec{w} = \vec{h}^{\vec{\kappa_1}} \textbf{ in } V) \textbf{ in letrec } z = h^{\kappa'}, \vec{w} = \vec{h}^{\vec{\kappa_1'}} \textbf{ in } M : \tau.$$

  By typing rules, we have

$$\begin{array}{l}(1)\Gamma_1 \vdash \textbf{letrec } z = h^{\kappa}, \vec{w} = \vec{h}^{\vec{\kappa_1}} \textbf{ in } V : \lceil \tau_1 \rceil \\ (2)\Gamma_2, x : \lceil \tau_1 \rceil \vdash \textbf{letrec } z = h^{\kappa'}, \vec{w} = \vec{h}^{\vec{\kappa_1'}} \textbf{ in } M : \tau \\ (3)\Gamma = \Gamma_1; \Gamma_2\end{array}$$

  By (1), (2) and typing rules, it must be that

$$\begin{array}{l}(4)\Gamma_1', z : \tau_z \vdash \textbf{letrec } \vec{w} = \vec{h}^{\vec{\kappa_1}} \textbf{ in } V : \lceil \tau_1 \rceil \\ (5)\Gamma_1'' \vdash z = h^{\kappa} : \tau_z \\ (6)\Gamma_2', x : \lceil \tau_1 \rceil, z : \tau_z' \vdash \textbf{letrec } \vec{w} = \vec{h}^{\vec{\kappa_1'}} \textbf{ in } M : \tau \\ (7)\Gamma_2'' \vdash z = h^{\kappa'} : \tau_z' \\ (8)\Gamma_1' + \Gamma_1'' = \Gamma_1 \\ (9)\Gamma_2' + \Gamma_2'' = \Gamma_2\end{array}$$

  By (4) and Lemma A.10, we have

$$(10)\lfloor \Gamma_1' \rfloor, z : \lfloor \tau_z \rfloor \vdash \textbf{letrec } \vec{w} = \vec{h}^{\lfloor \vec{\kappa_1} \rfloor} \textbf{ in } V : \lceil \tau_1 \rceil.$$

  By applying (T-Let) to (6) and (10), we obtain

$$\lfloor \Gamma_1' \rfloor; \Gamma_2', z : (\lfloor \tau_z \rfloor; \tau_z') \vdash \textbf{let } x = (\textbf{letrec } \vec{w} = \vec{h}^{\lfloor \vec{\kappa_1} \rfloor} \textbf{ in } V) \textbf{ in letrec } \vec{w} = \vec{h}^{\vec{\kappa_1'}} \textbf{ in } M : \tau.$$

  By induction hypothesis and (T-Weak), it follows that

$$(11)\lfloor \Gamma_1' \rfloor; \Gamma_2', z : (\lfloor \tau_z \rfloor + \tau_z') \vdash \textbf{letrec } \vec{w} = \vec{h}^{\lfloor \vec{\kappa_1} \rfloor; \vec{\kappa_1'}} \textbf{ in } [V/x]M : \tau.$$

By (5), (7), (11), Lemma A.8 and Lemma A.9, we have

$$(\lfloor \Gamma_1' \rfloor; \Gamma_2') + \lfloor \Gamma_1'' \rfloor + \Gamma_2'' \vdash \textbf{letrec } z = h^{\lfloor \kappa \rfloor + \kappa'}, \vec{w} = \vec{h}^{\lfloor \vec{\kappa_1} \rfloor; \vec{\kappa_1'}} \textbf{ in } [V/x]M : \tau.$$

By $(\lfloor \Gamma_1' \rfloor; \Gamma_2') + \lfloor \Gamma_1'' \rfloor + \Gamma_2'' = \lfloor \Gamma_1' \rfloor + \Gamma_2' + \lfloor \Gamma_1'' \rfloor + \Gamma_2'' \leq \lfloor \Gamma_1' + \Gamma_1'' \rfloor + (\Gamma_2' + \Gamma_2'') = \lfloor \Gamma_1 \rfloor + \Gamma_2 = \lfloor \Gamma_1 \rfloor; \Gamma_2 \leq \Gamma$, we have

$$\Gamma \vdash \textbf{letrec } z = h^{\lfloor \kappa \rfloor; \kappa'}, \vec{w} = \vec{h}^{\lfloor \vec{\kappa_1} \rfloor; \vec{\kappa_1'}} \textbf{ in } [V/x]M : \tau$$

as required.

□

Proof of Theorem 4.10: We show this by induction on the derivation of $D \xrightarrow{l} D'$ with case analysis on the last rule.

- (DR-Heap):

  In this case, $D = \textbf{let } x = h^{\kappa_1} \textbf{ in } M_2$, $D' = \textbf{letrec } x = h^{\kappa_1} \textbf{ in } M_2$, and $l = \epsilon$. Case for $h = \langle y_1, y_2 \rangle$ is trivial from typing rules. Suppose $h = \lambda y.M_1$ and $\Gamma \vdash D : \tau$. By the rule (T-Abs),

  $(1)\Gamma_1, y : \tau_1 \vdash M_1 : \tau_2$
  $(2)\Gamma_2, x : \tau_1 \to^{\kappa_1, \kappa_2} \tau_2 \vdash M_2 : \tau$
  $(3)\Gamma = \kappa_2 \lceil \Gamma_1 \rceil + \Gamma_2$

  Without loss of generality, we can assume that $x \notin dom(\Gamma_1)$. By applying (T-Weak) to (1), we have $(4)\Gamma_1, y : \tau_1, x : \tau_1 \to^{0,0} \tau_2 \vdash M_1 : \tau_2$. By (2), (4), (DT-Abs) and (DT-Heap), we have $\kappa_2(1+0)\lceil \Gamma_1 \rceil + \Gamma_2 \vdash D' : \tau$, that is, $\Gamma \vdash D' : \tau$.

- (DR-Rec): Trivial from the typing rules.

- (DR-Read): In this case, $(1)D = \textbf{letrec } x = h^{\kappa} \textbf{ in } D_1$, $(2)D' = \textbf{letrec } x = h^{\kappa - \kappa'} \textbf{ in } D_1'$, and $(3)D_1 \xrightarrow{x = h^{\kappa'}} D_1'$ for $h = \langle V_1, V_2 \rangle$ or $h = \lambda y.M_2$. Suppose $(4)\Gamma \vdash D : \tau$.

  - If $h = \langle V_1, V_2 \rangle$, then $(5)\Gamma = \Gamma_1 + V_1 : \tau_1 + V_2 : \tau_2$ and $(6)\Gamma_1, x : \tau_1 \times^{\kappa} \tau_2 \vdash D_1 : \tau$ for some Γ_1, τ_1, and τ_2. By Lemma A.6, there are some $\tau_1', \tau_1'', \tau_2', \tau_2''$ such that

    $(7)\tau_1 = \tau_1' + \tau_1''$
    $(8)\tau_2 = \tau_2' + \tau_2''$
    $(9)\Gamma_1 + V_1 : \tau_1' + V_2 : \tau_2', x : \tau_1'' \times^{\kappa - \kappa'} \tau_2'' \vdash D_1' : \tau.$

By (9), (DT-Pair) and (DT-Heap), (10)$\Gamma_1 + V_1 : \tau_1' + V_2 : \tau_2' + V_1 : \tau_1'' + V_2 : \tau_2'' \vdash$ **letrec** $x = \langle V_1, V_2 \rangle^{\kappa - \kappa'}$ **in** $D_1' : \tau$. Because $\Gamma_1 + V_1 : \tau_1' + V_2 : \tau_2' + V_1 : \tau_1'' + V_2 : \tau_2'' = \Gamma$ by (5), (7), and (8), $\Gamma \vdash$ **letrec** $x = \langle V_1, V_2 \rangle^{\kappa - \kappa'}$ **in** D_1'.

– If $h = \lambda^{\kappa} y.M_2$, then it must be that

(11)$\Gamma_1, y : \tau_1, x : \tau_1 \rightarrow^{\kappa_1, \kappa_2} \tau_2 \vdash M_2 : \tau_2$
(12)$\Gamma_2, x : \tau_1 \rightarrow^{\kappa_3, \kappa_4} \tau_2 \vdash D_1 : \tau$
(13)$\Gamma = \kappa_4(1 + \kappa_2)\lceil \Gamma_1 \rceil + \Gamma_2$
(14)$\kappa \geq \kappa_3(1 + \kappa_1), \kappa_3 \geq \delta, \kappa_4 \geq 1$

for some $\Gamma_1, \Gamma_2, \tau_1, \tau_2, \kappa_1, \kappa_2, \kappa_3$, and κ_4. By (3), (11), (12), and Lemma A.7, we have

(15)$\Gamma_2 + \Gamma_1, x : \tau_1 \rightarrow^{\kappa_1 + \kappa_3 - \kappa', \kappa_2 + \kappa_4 - 1} \tau_2 \vdash D_1' : \tau_3$

By (11), (15), (DT-Abs) and (DT-Heap),

$$(\kappa_2 + \kappa_4 - 1)(1 + \kappa_2)\lceil \Gamma_1 \rceil + (\Gamma_2 + \Gamma_1) \vdash \textbf{letrec } x = \lambda^{(\kappa_1 + \kappa_3 - \kappa')(1 + \kappa_1)} y.M_2 \textbf{ in } D_1' : \tau$$

The required condition $\Gamma \vdash$ **letrec** $x = \lambda^{\kappa - \kappa'} y.M_2$ **in** $D_1' : \tau$ follows if we show (a) $(\kappa_2 + \kappa_4 - 1)(1 + \kappa_2) + 1 \leq \kappa_4(1 + \kappa_2)$ and (b) $(\kappa_1 + \kappa_3 - \kappa')(1 + \kappa_1) \leq \kappa - \kappa'$. They can be shown as follows:

(a) The inequality is trivial if $\kappa_4(1 + \kappa_2) = \omega$. Otherwise, κ_2 must be 0 by (14). Then, $(\kappa_2 + \kappa_4 - 1)(1 + \kappa_2) + 1 = \kappa_4 - 1 + 1 = \kappa_4 = \kappa_4(1 + \kappa_2)$.

(b) The inequality is trivial if $\kappa = \omega$. Otherwise κ_1 must be 0 by (14). Then, $(\kappa_1 + \kappa_3 - \kappa')(1 + \kappa_1) = \kappa_3 - \kappa' = \kappa_3(1 + \kappa_1) - \kappa' \leq \kappa - \kappa'$.

- (DR-IfT):
In this case, $M =$ **if0** 0 **then** M_1 **else** M_2. Suppose $\Gamma \vdash M : \tau$. Then

$\Gamma_1 \vdash M_1 : \tau$
$\Gamma_1 \vdash M_2 : \tau$
$\Gamma_2 \vdash 0 : int$
$\Gamma = \Gamma_1 + \Gamma_2$

By (T-Weak), we have $\Gamma_1 + \Gamma_2 \vdash M_1 : \tau$, i.e., $\Gamma \vdash M' : \tau$.

- (DR-IfF): Similar to the case for (T-IfT).

- (DR-ConRec): In this case, $D =$ **letrec** $x = h^{\kappa}$ **in** D_1, $D' =$ **letrec** $x = h^{\kappa}$ **in** D_1', and $D_1 \xrightarrow{l} D_1'$. Suppose $\Gamma \vdash D : \tau$. Then, $\Gamma_1, x : \tau_1 \vdash D_1 : \tau$, $\Gamma_2 \vdash x = h^{\kappa} : \tau_1$, and $\Gamma = \Gamma_1 + \Gamma_2$ for some Γ_1 and Γ_2. Case analysis on l.

- Case $l = \epsilon$: By $D_1 \xrightarrow{\epsilon} D_1'$ and induction hypothesis, $\Gamma_1, x : \tau_1 \vdash D_1' : \tau$. So, by using (DT-Heap), we obtain $\Gamma \vdash D' : \tau$.
- Case $l = y$: By $D_1 \xrightarrow{y} D_1'$ and induction hypothesis, there exists D_1'' such that $\Gamma_1, x : \tau_1 \vdash D_1'' : \tau$ and $D_1 \xrightarrow{y} D_1''$. Let $D'' = \mathbf{letrec}\ x = h^{\kappa}\ \mathbf{in}\ D_1''$ Then, $D \xrightarrow{y} D''$ and $\Gamma \vdash D'' : \tau$.

- (DR-ConLet): In this case, $D = \mathbf{let}\ x = D_1\ \mathbf{in}\ D_2$, $D' = \mathbf{let}\ x = D_1'\ \mathbf{in}\ D_2$, and $D_1 \xrightarrow{l} D_1'$. Suppose $\Gamma \vdash D : \tau$. Then, by (T-Let), $\Gamma_1 \vdash D_1 : \tau_1$, $\Gamma_2, x : \tau_1 \vdash D_2 : \tau$, and $\Gamma = \Gamma_1; \Gamma_2$ for some Γ_1, Γ_2, and τ_1. Case analysis on l.
  - Case $l = \epsilon$: By $D_1 \xrightarrow{l} D_1'$ and induction hypothesis, $\Gamma_1 \vdash D_1' : \tau_1$. By using (T-Let), we obtain $\Gamma \vdash D' : \tau$.
  - Case $l = y$: By $D_1 \xrightarrow{y} D_1'$ and induction hypothesis, $\Gamma_1 \vdash D_1'' : \tau_1$ and $D_1 \xrightarrow{y} D_1''$ for some D_1''. Let $D'' = \mathbf{let}\ x = D_1''\ \mathbf{in}\ D_2$. Then $\Gamma \vdash D'' : \tau$ and $D \xrightarrow{y} D''$.

- (DR-Split): In this case, $D = \mathbf{letrec}\ x = h^{\kappa}\ \mathbf{in}\ \mathbf{let}\ y = D_1\ \mathbf{in}\ D_2$,
  $D' = \mathbf{let}\ y = (\mathbf{letrec}\ x = h^{\kappa_1}\ \mathbf{in}\ D_1)\ \mathbf{in}\ \mathbf{letrec}\ x = h^{\kappa_2}\ \mathbf{in}\ D_2$, and $\kappa = \kappa_1; \kappa_2$. Suppose $\Gamma \vdash D : \tau$. We show $\Gamma \vdash D'' : \tau$ and $D \xrightarrow{x} D''$ for some D'', by case analysis on h.
  - Case where h is of the form $\langle V_1, V_2 \rangle$.
    By (DT-Pair), (DT-Heap) and (T-Let), we have

    $$\begin{array}{l}\Gamma_1, x : \tau_1 \times^{\kappa_3} \tau_2 \vdash D_1 : \tau_3\\ \Gamma_2, x : \tau_4 \times^{\kappa_4} \tau_5, y : \tau_3 \vdash D_2 : \tau\\ \Gamma = (\Gamma_1; \Gamma_2) + V_1 : (\tau_1; \tau_4) + V_2 : (\tau_2; \tau_5)\\ \kappa = \kappa_3; \kappa_4\end{array}$$

    Let $D'' = \mathbf{let}\ y = (\mathbf{letrec}\ x = h^{\kappa_3}\ \mathbf{in}\ D_1)\ \mathbf{in}\ \mathbf{letrec}\ x = h^{\kappa_4}\ \mathbf{in}\ D_2$. Then, $D \xrightarrow{x} D''$ and

    $$(\Gamma_1 + V_1 : \tau_1 + V_2 : \tau_2); (\Gamma_2 + V_1 : \tau_4 + V_2 : \tau_5) \vdash D'' : \tau.$$

    Because $(\Gamma_1 + V_1 : \tau_1 + V_2 : \tau_2); (\Gamma_2 + V_1 : \tau_4 + V_2 : \tau_5) \leq (\Gamma_1; \Gamma_1) + V_1 : (\tau_1; \tau_4) + V_2 : (\tau_2; \tau_5) = \Gamma$, we have $\Gamma \vdash D'' : \tau$ by (T-Weak). (Here we used the law $(\Gamma_1 + \Gamma_2); (\Gamma_3 + \Gamma_4) \leq (\Gamma_1; \Gamma_3) + (\Gamma_2; \Gamma_4)$.
  - Case where h is of the form $\lambda z.M_3$.
    By (DT-Abs), (DT-Heap) and (T-Let), we have

    $$\begin{array}{l}\Gamma_1, x : \tau_1 \to^{\kappa_3, \kappa_4} \tau_2 \vdash D_1 : \tau_3\\ \Gamma_2, x : \tau_1 \to^{\kappa_5, \kappa_6} \tau_2, y : \tau_3 \vdash D_2 : \tau\\ \Gamma_3, x : \tau_1 \to^{\kappa_7, \kappa_8} \tau_2, z : \tau_1 \vdash M_3 : \tau\\ \Gamma = (\kappa_4; \kappa_6)(1 + \kappa_8)\lceil \Gamma_3 \rceil + (\Gamma_1; \Gamma_2)\\ \kappa \geq (\kappa_3; \kappa_5)(1 + \kappa_7)\end{array}$$

Since $(\kappa_3;\kappa_5)(1+\kappa_7) = (\kappa_3(1+\kappa_7));(\kappa_5(1+\kappa_7))$, we have κ_9, κ_{10} such that $\kappa = \kappa_9;\kappa_{10}$, $\kappa_9 \geq \kappa_3(1+\kappa_7)$, and $\kappa_{10} \geq \kappa_5(1+\kappa_7)$. Let $D'' = \textbf{let } y = (\textbf{letrec } x = h^{\kappa_9} \textbf{ in } D_1) \textbf{ in letrec } x = h^{\kappa_{10}} \textbf{ in } D_2$. Then, $D \xrightarrow{x} D''$. Moreover, by (T-Let), (DT-Abs) and (DT-Heap),

$$(\kappa_4(1+\kappa_8)\lceil\Gamma_3\rceil + \Gamma_1);(\kappa_6(1+\kappa_8)\lceil\Gamma_3\rceil + \Gamma_2) \vdash D'' : \tau$$

Because $(\kappa_4(1+\kappa_8)\lceil\Gamma_3\rceil + \Gamma_1);(\kappa_6(1+\kappa_8)\lceil\Gamma_3\rceil + \Gamma_2) \leq (\kappa_4(1+\kappa_8)\lceil\Gamma_3\rceil;\kappa_6(1+\kappa_8)\lceil\Gamma_3\rceil) + (\Gamma_1;\Gamma_2) = \Gamma$, we have $\Gamma \vdash D'' : \tau$ by (T-Weak).

- (DR-Var): This case follows from Lemma A.11.

□

A.4 Proof of Theorem 4.8

Lemma A.12: If $D \xrightarrow{x=h^{\kappa'}} D'$, $D^* = (H, M)$ and $D'^* = (H', M')$, then $(H + \{x \mapsto^{\kappa} h\}, M) \rightsquigarrow (H' + \{x \mapsto^{\kappa-\kappa'} h\}, M')$ for any κ such that $\kappa \geq \kappa'$.

Proof: Straightforward induction on the derivation of $D \xrightarrow{x=h^{\kappa'}} D'$. □

Lemma A.13: If $(H_1, M) \rightsquigarrow (H_1', M')$, then $(H_1; H_2, M) \rightsquigarrow (H, M')$ and $H \geq (H_1'; H_2)$ for some H.

Proof: Trivial from the fact that $H_1 = H_1'$ or $H_1 = H_3\{x \mapsto^{\kappa} h\} \wedge H_1' = H_3\{x \mapsto^{\kappa-\kappa'} h\}$. □

Lemma A.14: If $\textbf{letrec } \vec{x} = \vec{h}^{\vec{\kappa}} \textbf{ in } D_1 \uparrow$, then $\textbf{letrec } \vec{x} = \vec{h}^{\vec{\kappa}} \textbf{ in let } y = D_1 \textbf{ in } D_2 \uparrow$.

Proof: Suppose $\textbf{letrec } \vec{x} = \vec{h}^{\vec{\kappa}} \textbf{ in } D_1 \uparrow$. Then, $\textbf{letrec } \vec{x} = \vec{h}^{\vec{\kappa}} \textbf{ in let } y = D_1 \textbf{ in } D_2 \xrightarrow{\vec{x}} \textbf{let } y = (\textbf{letrec } \vec{x} = \vec{h}^{\vec{\kappa}} \textbf{ in } D_1) \textbf{ in } (\textbf{letrec } \vec{x} = \vec{h}^{\vec{0}} \textbf{ in } D_2) \xrightarrow{\hat{\epsilon}} \textbf{Error}$. ($\xrightarrow{\vec{x}}$ is a shorthand for $\xrightarrow{x_1} \cdots \xrightarrow{x_n}$.) Moreover, suppose $\textbf{letrec } \vec{x} = \vec{h}^{\vec{\kappa}} \textbf{ in let } y = D_1 \textbf{ in } D_2 \xrightarrow{\vec{x_2}} D' \xrightarrow{\epsilon} D''$. Then, it must be that

(1) $D' \equiv \textbf{letrec } \vec{x_1} = \vec{h_1}^{\vec{\kappa_1}} \textbf{ in let } y = \textbf{letrec } \vec{x_2} = \vec{h_2}^{\vec{\kappa_{21}}} \textbf{ in } D_1 \textbf{ in letrec } \vec{x_2} = \vec{h_2}^{\vec{\kappa_{22}}} \textbf{ in } D_2$

(2) $D'' \equiv \textbf{letrec } \vec{x_1} = \vec{h_1}^{\vec{\kappa_1}} \textbf{ in let } y = \textbf{letrec } \vec{x_2} = \vec{h_2}^{\vec{\kappa'_{21}}} \textbf{ in } D_1' \textbf{ in letrec } \vec{x_2} = \vec{h_2}^{\vec{\kappa_{22}}} \textbf{ in } D_2$

(3) $\textbf{letrec } \vec{x_2} = \vec{h_2}^{\vec{\kappa_{21}}} \textbf{ in } D_1 \xrightarrow{\epsilon} \textbf{letrec } \vec{x_2} = \vec{h_2}^{\vec{\kappa'_{21}}} \textbf{ in } D_1'$

(4) $\vec{x} = \vec{h}^{\vec{\kappa}} \equiv (\vec{x_1} = \vec{h_1}^{\vec{\kappa_1}}, \vec{x_2} = \vec{h_2}^{\vec{\kappa_{21}};\vec{\kappa_{22}}})$.

The conditions (3) and (4) contradicts with $\textbf{letrec } \vec{x} = \vec{h}^{\vec{\kappa}} \textbf{ in } D_1 \uparrow$. (We can easily construct a derivation for $\textbf{letrec } \vec{x} = \vec{h}^{\vec{\kappa}} \textbf{ in } D_1 \xrightarrow{\epsilon} \textbf{letrec } \vec{x} = \vec{h}^{\vec{\kappa'}} \textbf{ in } D_1'$ from (3).) □

Proof of Theorem 4.8:

1. Because $D \xrightarrow{x} D'$ implies $D^* = D'^*$, it suffices to show that $D \xrightarrow{\epsilon} D'$ implies that $D^* \rightsquigarrow (H, M)$ and $(H, M) \geq D'^*$ hold for some H, M. We show it by induction on the derivation of $D \xrightarrow{\epsilon} D'$, with case analysis on the last rule.

   Cases for (DR-Heap), (DR-Rec), (DR-IfT), (DR-IfF), (DR-ConRec), and (DR-Var) are trivial. Case for (DR-Read) follows from Lemma A.12.

   If the last rule is (DR-ConLet), we have $(1)D \equiv \textbf{let } x = D_1 \textbf{ in } D_2$, $(2)D' \equiv \textbf{let } x = D_1' \textbf{ in } D_2$, $(3)D_1 \xrightarrow{\epsilon} D_1'$, $(4)D_1^* = (H_1, M_1)$, $(5)D_2^* = (H_2, M_2)$, and $(6)D^* = (H_1; H_2, \textbf{let } x = M_1 \textbf{ in } M_2)$. By (3), (4), and induction hypothesis, there are H_1', M_1' such that $(7)(H_1, M_1) \rightsquigarrow (H_1', M_1')$ and $(8)D_1'^* \leq (H_1', M_1')$. By (6), (7), and Lemma A.13, $D^* \rightsquigarrow (H', \textbf{let } x = M_1' \textbf{ in } M_2)$ and $(9)H' \geq (H_1'; H_2)$ for some H'. By (2), (5), (8), and (9), we have $D'^* \leq (H', \textbf{let } x = M_1' \textbf{ in } M_2)$ as required.

2. Suppose $(1)(H, M) \rightsquigarrow \textbf{Error}$ and $(2)(H, M) \geq D^*$. By reduction rules, $(3)M \equiv C[I]$ for some context $C[\ ]$ and expression I of the form $apply^\kappa(x, V)$, $\textbf{fst}^\kappa(x)$, or $\textbf{snd}^\kappa(x)$. We can easily show $D \uparrow$ by induction on the structure of $C[\ ]$.

   - Case $C[\ ] \equiv [\ ]$: Straightfoward case analysis on I.
   - Case $C[\ ] \equiv \textbf{let } x = C'[\ ] \textbf{ in } M_2$:

     $$(5)D \equiv \textbf{letrec } \vec{y} = \vec{h_y}^{\vec{\kappa_y}} \textbf{ in } (\textbf{let } x = \textbf{letrec } \vec{z} = \vec{h_z}^{\vec{\kappa_{z1}}}, \vec{w} = \vec{h_w}^{\vec{\kappa_w}} \textbf{ in } C'[I] \textbf{ in } \textbf{letrec } \vec{z} = \vec{h_z}^{\vec{\kappa_{z2}}} \textbf{ in } M_1)$$
     $$(6)H \geq \{\vec{y} \mapsto^{\vec{\kappa_y}} \vec{h_y}, \vec{z} \mapsto^{\vec{\kappa_{z1}};\vec{\kappa_{z2}}} \vec{h_z}, \vec{w} \mapsto^{\vec{\kappa_w}} \vec{h_w}\}.$$

     Let $D_1 = \textbf{letrec } \vec{y} = \vec{h_y}^{\vec{\kappa_y}}, \vec{z} = \vec{h_z}^{\vec{\kappa_{z1}}}, \vec{w} = \vec{h_w}^{\vec{\kappa_w}} \textbf{ in } C'[I]$. Then by induction hypothesis, $D_1 \uparrow$. By Lemma A.14, $D \uparrow$.

3. Suppose $(1)(H, M) \rightsquigarrow (H', M')$ and $(2)(H, M) \geq D^*$. By reduction rules, $(3)M \equiv C[I]$ and $(4)M' \equiv C[M_1]$ for some context $C[\ ]$ and expression I of the form $\textbf{let } x = h^\kappa \textbf{ in } M_2$, $\textbf{let } x = \textbf{rec}^\kappa(f, y, M_2) \textbf{ in } M_3$, $\textbf{let } x = V \textbf{ in } M$, $apply^\kappa(x, V)$, $\textbf{fst}^\kappa(x)$, $\textbf{snd}^\kappa(x)$, or $\textbf{if0 } n \textbf{ then } M_2 \textbf{ else } M_3$. We show that either $D \uparrow$ holds or there exists D' such that $D \xrightarrow{\hat{\epsilon}} D'$ and $(H', M') \geq D'^*$ by induction on the structure of $C[\ ]$.

   - Case $C[\ ] = [\ ]$: Straightfoward case analysis on I.

- Case $C[\ ] = \textbf{let}\ x = C'[\ ]\ \textbf{in}\ M_2$: By (2), it must be that

$$(5) D \equiv \textbf{letrec}\ \vec{y} = \vec{h_y}^{\vec{\kappa_y}}\ \textbf{in}\ (\textbf{let}\ x = \textbf{letrec}\ \vec{z} = \vec{h_z}^{\vec{\kappa_{z1}}}, \vec{w} = \vec{h_w}^{\vec{\kappa_w}}\ \textbf{in}\ C'[I]\ \textbf{in}\ \textbf{letrec}\ \vec{z} = \vec{h_z}^{\vec{\kappa_{z2}}}\ \textbf{in}\ M_1)$$
$$(6) H \geq \{\vec{y} \mapsto^{\vec{\kappa_y}} \vec{h_y}, \vec{z} \mapsto^{\vec{\kappa_{z1}};\vec{\kappa_{z2}}} \vec{h_z}, \vec{w} \mapsto^{\vec{\kappa_w}} \vec{h_w}\}.$$

Let $H_1 = \{\vec{y} \mapsto^{\vec{\kappa_y}} \vec{h_y}, \vec{z} \mapsto^{\vec{\kappa_{z1}}} \vec{h_z}, \vec{w} \mapsto^{\vec{\kappa_w}} \vec{h_w}\}$ and $D_1 = \textbf{letrec}\ \vec{y} = \vec{h_y}^{\vec{\kappa_y}}, \vec{z} = \vec{h_z}^{\vec{\kappa_{z1}}}, \vec{w} = \vec{h_w}^{\vec{\kappa_w}}\ \textbf{in}\ C'[I]$ Then, by (3) and (4), either $(H_1, C'[I]) \rightsquigarrow (H_1', C'[M_1])$ and $H' \geq H_1'; \{\vec{z} \mapsto^{\vec{\kappa_{z2}}} \vec{h_z}\}$, or $(H_1, C'[I]) \rightsquigarrow \textbf{Error}$. In the latter case, $D_1 \uparrow$ by the second property of the theorem. By Lemma A.14, $D \uparrow$. In the former case, by the induction hypothesis, $D_1 \xrightarrow{\hat{\epsilon}} D_1'$ and $(H_1', C'[M_1]) \geq D_1'^*$. Let $D' = \textbf{let}\ x = D_1'\ \textbf{in}\ \textbf{letrec}\ \vec{y} = \vec{h_y}^{\vec{0}}, \vec{z} = \vec{h_z}^{\vec{\kappa_{z2}}}\ \textbf{in}\ M_1$. Then, $D \xrightarrow{\hat{\epsilon}} D'$ and $(H', M') \geq D'^*$.

□