Fractional Ownerships
for Safe Memory Deallocation

Naoki Kobayashi and Kohei Suenaga

Tohoku University

Abstract. We propose a type system for a programming language with memory allocation/deallocation primitives, which prevents memory-related errors such as double-frees and memory leaks. The key idea is to augment pointer types with fractional ownerships, which express both capabilities and obligations to access or deallocate memory cells. Thanks to the use of fractions as ownerships, the type system admits a polynomial-time type inference algorithm, which serves as an algorithm for automatic verification of lack of memory-related errors. A prototype verifier has been implemented and tested for several programs manipulating lists, trees, and doubly-linked lists.

1   Introduction

In programming languages with manual memory management (like C and C++), a misuse of memory allocation/deallocation primitives often causes serious, hard-to-find bugs. We propose a new type system for statically preventing such memory-related errors. More precisely, the type system prevents memory leaks (forgetting to deallocate memory cells), double frees (deallocating memory cells more than once), and read/write accesses to deallocated memory. The type system is equipped with a polynomial-time type inference algorithm, so that programs can be automatically verified.

The key idea of our type system is to assign *fractional ownerships* to pointer types. An ownership ranges over the set of rational numbers in $[0, 1]$, and expresses both a capability (or permission) to access a pointer, and an obligation to deallocate the memory referred to by the pointer. As in Boyland's fractional permissions [1], a non-zero ownership expresses a permission to dereference the pointer, and an ownership of 1 expresses a permission to update the memory cell referenced by the pointer. In addition, a non-zero ownership expresses an obligation to eventually deallocate (the cell referenced by) the pointer, and an ownership of 1 also expresses a permission to deallocate the pointer. (Therefore, if one has an ownership of 0.5, one has to eventually combine it with other ownerships to obtain an ownership of 1, to fulfill the obligation to deallocate the pointer).

For example, **int ref$_1$ ref$_1$** is the type of a pointer to an pointer to an integer, such that both the pointers can be read/written, and must be deallocated through the pointer. **int ref$_0$ ref$_1$** is the type of a pointer to an pointer to

Fig. 1. List-like structure

an integer, such that only the first pointer can be read/written, and must be deallocated. To see how such types can be used, consider the following program, written in an ML-like language (but with memory deallocation primitive `free`).

```
fun freeall(x) =                freeall : μα.(α ref₁) → μα.(α ref₀)
   if null(x)                   x : μα.(α ref₁)
   then skip                    x : μα.(α ref₀)
   else let y = *x in           x : μα.(α ref₁)
         (freeall(y);           x : (μα.(α ref₀)) ref₁, y : μα.(α ref₁)
          free(x)               x : (μα.(α ref₀)) ref₁, y : μα.(α ref₀)
         )                      x : μα.(α ref₀), y : μα.(α ref₀)
```

The function `freeall` takes as an argument a pointer `x` to a list structure shown in Figure 1, and deallocates all the pointers reachable from `x`. The right-hand side shows the type of function `freeall`, as well as the types assigned to `x` and `y` before execution of each line. (Our type system is flow-sensitive, so that different types are assigned at different program points.) Here, $\mu\alpha.\tau$ is a recursive type. In the type of `freeall` on the first line, $\mu\alpha.(\alpha\ \mathbf{ref}_1)$ and $\mu\alpha.(\alpha\ \mathbf{ref}_0)$ are the types of x before and after the call of the function. The type $\mu\alpha.(\alpha\ \mathbf{ref}_1)$ means that the argument `x` must hold the ownerships of all the pointers reachable from `x` when the function is called, while $\mu\alpha.(\alpha\ \mathbf{ref}_0)$ means that `x` holds no ownerships when the function returns (which implies that all the pointers reachable from `x` will be deallocated inside the function).

The type assignment at the beginning of the function indicates that all the memory cells reachable from `x` should be deallocated through variable `x`. In the then-branch, `x` is a null pointer, so that all the ownerships are cleared to 0. In the else-branch, **let** $y = *x$ **in** $\cdots$ transfers a part of the ownerships held by `x` to `y`; after that, `x` has type $(\mu\alpha.(\alpha\ \mathbf{ref}_0))\ \mathbf{ref}_1$, indicating that x holds only the ownership of the pointer stored in `x`. The other ownerships (of the pointers that are reachable from `x`) are now held by `y`. After the recursive call to `freeall`, all the ownerships held by `y` become empty. Finally, after `free(x)`, the ownership of `x` also becomes empty.

The type system with fractional ownerships prevents: (i) memory leaks by maintaining the invariant that the total ownership for each memory cell is 1 until the cell is deallocated and by ensuring the ownerships held by a variable are empty at the end of the scope of the variable, (ii) double frees by ensuring that the ownership for a cell is consumed when the cell is deallocated, and (iii) illegal access to deallocated cells by requiring that a non-zero ownership is required for read/write operations.

Based on the type system, we have implemented a prototype verifier, and tested it for programs manipulating lists, trees, and doubly-linked lists.

Ownerships are also used in Heine and Lam's static analysis for detecting memory leaks [3]. Major differences are:

– In their system [3], a variable can hold only the ownership of the pointer stored in the variable, while in our type system, a variable can hold ownerships of any pointers reachable from the variable. In their system, therefore, an ownership cannot be passed to a pointer to a pointer or an array of pointers; for the example above, they cannot express a type like $\mu\alpha.\alpha\ \mathbf{ref}_1$, which holds all the ownerships of the reachable cells. Because of this restriction, we believe their system cannot verify list-manipulating C programs like the one given above.
– Their ownerships are integer-valued, while ours are fractions. Thus, the ownership (or type) inference is reduced to integer linear programming (which is NP-hard in general) in their type system, while in our type system, it is reduced to linear programming over rational numbers, which is solved in polynomial time.
– Their system does not prevent illegal access to deallocated pointers (in fact, no ownership is required for read/write operations in their system).

The rest of this paper is structured as follows. Section 2 introduces a simple imperative language that has only pointers as values. Section 3 presents our type system with fractional ownerships, proves its soundness, and discusses type inference issues. Section 4 discusses extensions to deal with data structures. Section 5 reports a prototype implementation of our type-based verification algorithm. Section 6 discusses related work and Section 7 concludes.

2 Language

This section introduces a simple imperative language with primitives for memory allocation/deallocation. For the sake of simplicity, the only values are (possibly null) pointers. See Section 4 for extensions of the language and the type system to deal with other language constructs.

The syntax of the language is given as follows.

Definition 1 (commands, programs)

s *(commands)* $::= \mathbf{skip} \mid {*}x \leftarrow y \mid s_1; s_2 \mid \mathbf{free}(x) \mid \mathbf{let}\ x = \mathbf{malloc}()\ \mathbf{in}\ s$
$\qquad\qquad\qquad\quad \mid \mathbf{let}\ x = \mathbf{null}\ \mathbf{in}\ s \mid \mathbf{let}\ x = y\ \mathbf{in}\ s \mid \mathbf{let}\ x = {*}y\ \mathbf{in}\ s$
$\qquad\qquad\qquad\quad \mid \mathbf{ifnull}(x)\ \mathbf{then}\ s_1\ \mathbf{else}\ s_2 \mid f(x_1,\ldots,x_n)$
$\qquad\qquad\qquad\quad \mid \mathbf{assert}(x = y) \mid \mathbf{assert}(x = {*}y)$
d *(definitions)* $::= f(x_1,\ldots,x_n) = s$

A program is a pair (D, s), where D is a set of definitions.

The command **skip** does nothing. ${*}x \leftarrow y$ updates the target of x (i.e., the contents of the memory cell pointed to by x) with the value of y. The command $s_1; s_2$ is a sequential execution of s_1 and s_2. The command $\mathbf{free}(x)$ deallocates

(the cell referenced by) the pointer x. The command **let** $x = e$ **in** s evaluates e, binds x to the value of e, and executes s. The expression **malloc**() allocates a memory cell and returns a pointer to it. The expression **null** denotes a null pointer. $*y$ dereferences the pointer y. The command **ifnull**(x) **then** s_1 **else** s_2 executes s_1 if x is null, and executes s_2 otherwise. The command $f(x_1, \ldots, x_n)$ calls function f. We require that $x_1, \ldots, x_n$ are mutually distinct variables. (This does not lose generality, as we can replace $f(x, x)$ with **let** $y = x$ **in** $f(x, y)$.) There is no return value of a function call; values can be returned only by reference passing. The commands **assert**$(x = y)$ and **assert**$(x = *y)$ do nothing if the equality holds, and aborts the program otherwise. These are used as guides for our type-based analysis described in the next section. Usually, they can be automatically inserted during the transformation from a surface language (like C) into our language; for example, **assert**$(x = y)$ is automatically inserted at the end of a let-expression **let** $x = y$ **in** $\cdots$. Separate pointer analyses may also be used to insert assertions; in general, insertion of more assertions makes our analysis more precise.

Remark 1. Notice that unlike in C (and like in functional languages), variables are immutable; they are initialized in let-expressions, and are never re-assigned afterwards. The declaration `int x = 1; ...` in C is expressed as:

$$\textbf{let } \&x = \textbf{malloc}() \textbf{ in } (*\&x \leftarrow 1; \cdots; \textbf{free}(\&x))$$

in our language. Here, $\&x$ is treated as a variable name.

Operational Semantics We assume that there is a countable set $\mathcal{H}$ of *heap addresses*. A run-time state is represented by a triple $\langle H, R, s \rangle$, where H is a mapping from a finite subset of $\mathcal{H}$ to $\mathcal{H} \cup \{\textbf{null}\}$, R is a mapping from a finite set of variables to $\mathcal{H} \cup \{\textbf{null}\}$. Intuitively, H models the heap memory, and R models local variables stored in stacks or registers. The set of *evaluation contexts* is defined by $E ::= [] \mid E; s$. We write $E[s]$ for the command obtained by replacing $[]$ in E with s.

Figure 2 shows main rules for the transition of run-time states: See Appendix A for the other rules. In the figure, $f\{x \mapsto v\}$ denotes the function f' such that $dom(f) = dom(f') \cup \{x\}$, $f'(x) = v$, and $f'(y) = f(y)$ for every $y \in dom(f) \setminus \{x\}$. $[x'/x]s$ denotes the command obtained by replacing x in s with x'. $\tilde{x}$ abbreviates a sequence $x_1, \ldots, x_n$. In the rules for let-expressions, we require that $x' \notin dom(R)$. In the rule for malloc, the contents v of the allocated cell can be any value in $\mathcal{H} \cup \{\textbf{null}\}$. There are three kinds of run-time errors: **NullEx** for accessing null pointers, **Error** for illegal read/write/free operations on deallocated pointers, and **AssertFail** for assertion failures. The type system in this paper will prevent only the errors expressed by **Error**.

Note that the function call $f(x_1, \ldots, x_n)$ is just replaced by the function's body. Thus, preprocessing is required to handle functions in C: A function call `x = f(y)` in C is simulated by $f(y, \&x)$ in our language (where $\&x$ is a variable name), and a C function definition `f(y) {s; return v;}` is simulated by:

$$f(y, r) = \textbf{let } \&y = \textbf{malloc}() \textbf{ in } (*\&y \leftarrow y; s; *r \leftarrow v; \textbf{free}(\&y)).$$

$$\frac{R(x) \in dom(H)}{\langle H, R, E[*x \leftarrow y] \rangle \longrightarrow_D \langle H\{R(x) \mapsto R(y)\}, R, E[\mathbf{skip}] \rangle}$$

$$\frac{R(x) \in dom(H) \cup \{\mathbf{null}\}}{\langle H, R, E[\mathbf{free}(x)] \rangle \longrightarrow_D \langle H \setminus \{R(x)\}, R, E[\mathbf{skip}] \rangle}$$

$$\frac{}{\langle H, R, E[\mathbf{let}\ x = y\ \mathbf{in}\ s] \rangle \longrightarrow_D \langle H, R\{x' \mapsto R(y)\}, E[[x'/x]s] \rangle}$$

$$\frac{}{\langle H, R, E[\mathbf{let}\ x = *y\ \mathbf{in}\ s] \rangle \longrightarrow_D \langle H, R\{x' \mapsto H(R(y))\}, E[[x'/x]s] \rangle}$$

$$\frac{h \notin dom(H)}{\langle H, R, E[\mathbf{let}\ x = \mathbf{malloc}()\ \mathbf{in}\ s] \rangle \longrightarrow_D \langle H\{h \mapsto v\}, R\{x' \mapsto h\}, E[[x'/x]s] \rangle}$$

$$\frac{}{\langle H, R\{x \mapsto \mathbf{null}\}, E[\mathbf{ifnull}(x)\ \mathbf{then}\ s_1\ \mathbf{else}\ s_2] \rangle \longrightarrow_D \langle H, R\{x \mapsto \mathbf{null}\}, E[s_1] \rangle}$$

$$\frac{f(\tilde{y}) = s \in D}{\langle H, R, E[f(\tilde{x})] \rangle \longrightarrow_D \langle H, R, E[[\tilde{x}/\tilde{y}]s] \rangle}$$

$$\frac{R(x) = H(R(y))}{\langle H, R, E[\mathbf{assert}(x = *y)] \rangle \longrightarrow_D \langle H, R, E[\mathbf{skip}] \rangle}$$

$$\frac{R(x) = \mathbf{null}}{\langle H, R, E[*x \leftarrow y] \rangle \longrightarrow_D \mathbf{NullEx}} \qquad \frac{R(y) = \mathbf{null}}{\langle H, R, E[\mathbf{let}\ x = *y\ \mathbf{in}\ s] \rangle \longrightarrow_D \mathbf{NullEx}}$$

$$\frac{R(x) \notin dom(H) \cup \{\mathbf{null}\}}{\langle H, R, E[*x \leftarrow y] \rangle \longrightarrow_D \mathbf{Error}} \qquad \frac{R(y) \notin dom(H) \cup \{\mathbf{null}\}}{\langle H, R, E[\mathbf{let}\ x = *y\ \mathbf{in}\ s] \rangle \longrightarrow_D \mathbf{Error}}$$

$$\frac{R(x) \notin dom(H) \cup \{\mathbf{null}\}}{\langle H, R, E[\mathbf{free}(x)] \rangle \longrightarrow_D \mathbf{Error}} \qquad \frac{R(y) \notin dom(H) \vee R(x) \neq H(R(y))}{\langle H, R, E[\mathbf{assert}(x = *y)] \rangle \longrightarrow_D \mathbf{AssertFail}}$$

Fig. 2. Main Transition Rules

Here, the malloc and free commands above correspond to the allocation and deallocation of a stack frame.

3 Type System

This section introduces a type system that prevents memory leaks, double frees, and illegal read/write operations.

3.1 Types

The syntax of types is given by:

$$\tau\ \text{(value types)} ::= \alpha \mid \tau\ \mathbf{ref}_f \mid \mu\alpha.\tau$$
$$\sigma\ \text{(function types)} ::= (\tau_1, \ldots, \tau_n) \to (\tau_1', \ldots, \tau_n')$$

We often write $\top$ for $\mu\alpha.\alpha$. The metavariable f ranges over rational numbers in $[0, 1]$. f, called an *ownership*, represents both a capability and an obligation to read/write/free a pointer.

α is a type variable, which gets bound by the recursive type constructor $\mu\alpha$. The type $\tau\ \mathbf{ref}_f$ describes a pointer whose ownership is f, and also expresses

the constraint that the value obtained by dereferencing the pointer should be used according to τ. For example, if x has type $\top \mathbf{ref}_1 \mathbf{ref}_1$, not only the pointer x but also the pointer stored in the target of the pointer x must be eventually deallocated through x.

Type $(\tau_1, \ldots, \tau_n) \rightarrow (\tau_1', \ldots, \tau_n')$ describes a function that takes n arguments. The types $\tau_1, \ldots, \tau_n, \tau_1', \ldots, \tau_n'$ describe how ownerships on arguments are changed by the function: the type of the i-th argument is τ_i at the beginning of the function, and it is τ_i' at the end of the function. (Recall the example in Section 1.)

The semantics of (value) types is defined as a mapping from the set $\{0\}^*$ (the set of finite sequences of the symbol 0) to the set of rational numbers.

Definition 2 *The mapping $[\![\cdot]\!]$ from the set of closed types to $\{0\}^* \rightarrow [0,1]$ is the least function that satisfies the following conditions.*

$$[\![\tau\ \mathbf{ref}_f]\!](\epsilon) = f \qquad [\![\tau\ \mathbf{ref}_f]\!](0w) = [\![\tau]\!](w) \qquad [\![\mu\alpha.\tau]\!] = [\![[\mu\alpha.\tau/\alpha]\tau]\!]$$

(Here, the order between functions from S to T is defined by: $f \leq_{S \rightarrow T} g$ if and only if $\forall x \in S.f(x) \leq_T g(x)$.) We write $\tau \approx \tau'$, if $[\![\tau]\!] = [\![\tau']\!]$.

Note that $\top(= \mu\alpha.\alpha) \approx \mu\alpha.(\alpha\ \mathbf{ref}_0)$, and $\mu\alpha.\tau \approx [\mu\alpha.\tau/\alpha]\tau$.

We write $\mathbf{empty}(\tau)$ if all the ownerships in τ are 0. We say that a type τ is *well-formed* if $[\![\tau]\!](w) \geq c \times [\![\tau]\!](w0)$ for every $w \in \{0\}^*$. Here, we let c be the constant $1/2$, but the type system given below remains sound as long as c is a positive (rational) number. In the rest of this paper, we consider only types that satisfy the well-formedness condition. See Remark 2 for the reason why the well-formedness is required.

3.2 Typing

A type judgment is of the form $\Theta; \Gamma \vdash s \Rightarrow \Gamma'$, where Θ is a finite mapping from (function) variables to function types, Γ and Γ' are finite mappings from variables to value types. Γ describes the ownerships held by each variable before the execution of s, while Γ' describes the ownerships after the execution of s. For example, we have $\Theta; x : \top \mathbf{ref}_1 \vdash \mathbf{free}(x) \Rightarrow x : \top \mathbf{ref}_0$. Note that a variable's type describes how the variable should be used, and not necessarily the status of the value stored in the variable. For example, $x : \top \mathbf{ref}_0$ does not mean that the memory cell pointed to by x has been deallocated; it only means that deallocating the cell through x (i.e., executing $\mathbf{free}(x)$) is disallowed. There may be another variable y of type $\tau \mathbf{ref}_1$ that holds the same pointer as x.

Typing rules are shown in Figure 3. $\tau \approx \tau_1 + \tau_2$ and $\tau_1 + \tau_2 \approx \tau_1' + \tau_2'$ mean $[\![\tau]\!] = [\![\tau_1]\!] + [\![\tau_2]\!]$ and $[\![\tau_1]\!] + [\![\tau_2]\!] = [\![\tau_1']\!] + [\![\tau_2']\!]$ respectively. In the rule for assignment $*x \leftarrow y$, we require that the ownership of x is 1 (see Remark 2). The ownerships of τ' must be empty, since the value stored in $*x$ is thrown away by the assignment. The ownerships of y (described by τ) is divided into τ_1, which will be transferred to x, and τ_2, which remains in y.

In the rule for **free**, the ownership of x is changed from 1 to 0. τ must be empty, since x can no longer be dereferenced. In the rule for **malloc**, the ownership of x is 1 at the beginning of s, indicating that x must be deallocated. At the end of s, we require that the ownership of x is 0, since x goes out of the scope. Note that this requirement does not prevent the allocated memory cell from escaping the scope of the let-expression: For example, **let** $x = $ **malloc**() **in** $*y \leftarrow x$ allows the new cell to escape through variable y. The ownership of x is empty at the end of the let-expression, since the ownership has been transferred to y.

In the rule for dereferencing (**let** $x = *y$ **in** $\cdots$), the ownership of y must be non-zero. The ownerships stored in the target of the pointer y, described by τ, are divided into τ_1 and τ_2. At the end of the let-expression, the ownerships held by x must be empty (which is ensured by **empty**(τ_1')), since x goes out of scope.

In the rule for **null**, there is no constraint on the type of x, since x is a null pointer. In the rule for conditionals, any type may be assigned to x in the then-branch. Thanks to this, **ifnull**(x) **then skip else free**(x) is typed as follows.

$$\frac{\Theta; x : \top \; \mathbf{ref}_0 \vdash \mathbf{skip} \Rightarrow x : \top \; \mathbf{ref}_0 \qquad \Theta; x : \top \; \mathbf{ref}_1 \vdash \mathbf{free}(x) \Rightarrow x : \top \; \mathbf{ref}_0}{\Theta; x : \top \; \mathbf{ref}_1 \vdash \mathbf{ifnull}(x) \; \mathbf{then} \; \mathbf{skip} \; \mathbf{else} \; \mathbf{free}(x) \Rightarrow x : \top \; \mathbf{ref}_0}$$

The rules for assertions allow us to shuffle the ownerships held by the same pointers.

Remark 2. The well-formedness condition approximates the condition: $\forall w \in \{0\}^*.([\![\tau]\!](w) = 0 \Rightarrow [\![\tau]\!](w0) = 0)$. Types that violate the condition (like $(\top \; \mathbf{ref}_1) \; \mathbf{ref}_0$) make the type system unsound. For example, consider the following command s (here, some let-expressions are inlined):

$$\mathbf{let} \; y = x \; \mathbf{in} \; (*y \leftarrow \mathbf{null}; \mathbf{assert}(x = y); \mathbf{free}(*x); \mathbf{free}(x)).$$

If we ignore the well-formedness condition, we can derive $\Theta; x : (\top \; \mathbf{ref}_1) \; \mathbf{ref}_1 \vdash s \Rightarrow x : (\top \; \mathbf{ref}_0) \; \mathbf{ref}_0$ from $\Theta; x : (\top \; \mathbf{ref}_1) \; \mathbf{ref}_0, y : (\top \; \mathbf{ref}_0) \; \mathbf{ref}_1 \vdash s' \Rightarrow x:(\top \; \mathbf{ref}_0) \; \mathbf{ref}_0, y:(\top \; \mathbf{ref}_0) \; \mathbf{ref}_0$ where s' is the body of s. However, the judgment is semantically wrong: the memory cell referenced by $*x$ is not deallocated by s (see Figure 4). The well-formedness condition ensures that if a variable (say, x) has an ownership of a pointer (say, p) reachable from x, then the variable must hold a fraction of ownerships for all the pointers between x and p, so that the pointers cannot be updated through aliases.

Example 1. Recall the example in Section 1. The part **let** $y = *x$ **in** (`freeall`(y); **free**(x)) is typed as follows.

$$\frac{\Theta; x : \tau, y : \mu\alpha.(\alpha \; \mathbf{ref}_1) \vdash \mathtt{freeall}(y) \Rightarrow x : \tau, y : \top \qquad \Theta; x : \tau, y : \top \vdash \mathbf{free}(x) \Rightarrow x : \top, y : \top}{\dfrac{\Theta; x : (\mu\alpha.(\alpha \; \mathbf{ref}_0)) \; \mathbf{ref}_1, y : \mu\alpha.(\alpha \; \mathbf{ref}_1) \vdash (\mathtt{freeall}(y); \mathbf{free}(x)) \Rightarrow x : \top, y : \top}{\Theta; x : \mu\alpha.(\alpha \; \mathbf{ref}_1) \vdash \mathbf{let} \; y = *x \; \mathbf{in} \; (\mathtt{freeall}(y); \mathbf{free}(x)) \Rightarrow x : \top}}$$

Here, $\tau = (\mu\alpha.(\alpha \; \mathbf{ref}_0)) \; \mathbf{ref}_1$ and $\Theta = \mathtt{freeall} : (\mu\alpha.(\alpha \; \mathbf{ref}_1)) \rightarrow (\top)$.

$$\overline{\Theta; \Gamma \vdash \mathbf{skip} \Rightarrow \Gamma} \qquad \text{(T-SKIP)}$$

$$\frac{\tau \approx \tau_1 + \tau_2 \qquad \mathbf{empty}(\tau')}{\Theta; \Gamma, x : \tau' \, \mathbf{ref}_1, y : \tau \vdash *x \leftarrow y \Rightarrow \Gamma, x : \tau_1 \, \mathbf{ref}_1, y : \tau_2} \qquad \text{(T-ASSIGN)}$$

$$\frac{\mathbf{empty}(\tau)}{\Theta; \Gamma, x : \tau \, \mathbf{ref}_1 \vdash \mathbf{free}(x) \Rightarrow \Gamma, x : \tau \, \mathbf{ref}_0} \qquad \text{(T-FREE)}$$

$$\frac{\Theta; \Gamma \vdash s_1 \Rightarrow \Gamma'' \qquad \Gamma'' \vdash s_2 \Rightarrow \Gamma'}{\Theta; \Gamma \vdash s_1 ; s_2 \Rightarrow \Gamma'} \qquad \text{(T-SEQ)}$$

$$\frac{\Theta; \Gamma, x : \tau \vdash s \Rightarrow \Gamma', x : \tau'}{\Theta; \Gamma \vdash \mathbf{let} \; x = \mathbf{null} \; \mathbf{in} \; s \Rightarrow \Gamma'} \qquad \text{(T-NULL)}$$

$$\frac{\Theta; \Gamma, x : \tau_1, y : \tau_2 \vdash s \Rightarrow \Gamma', x : \tau_1' \qquad \tau \approx \tau_1 + \tau_2 \qquad \mathbf{empty}(\tau_1')}{\Theta; \Gamma, y : \tau \vdash \mathbf{let} \; x = y \; \mathbf{in} \; s \Rightarrow \Gamma'} \qquad \text{(T-LET)}$$

$$\frac{\Theta; \Gamma, x : \tau_1, y : \tau_2 \, \mathbf{ref}_f \vdash s \Rightarrow \Gamma', x : \tau_1' \qquad f > 0 \qquad \tau \approx \tau_1 + \tau_2 \qquad \mathbf{empty}(\tau_1')}{\Theta; \Gamma, y : \tau \, \mathbf{ref}_f \vdash \mathbf{let} \; x = *y \; \mathbf{in} \; s \Rightarrow \Gamma'} \qquad \text{(T-LET*)}$$

$$\frac{\Theta; \Gamma, x : \tau \, \mathbf{ref}_1 \vdash s \Rightarrow \Gamma', x : \tau' \, \mathbf{ref}_0 \qquad \mathbf{empty}(\tau) \qquad \mathbf{empty}(\tau')}{\Theta; \Gamma \vdash \mathbf{let} \; x = \mathbf{malloc}() \; \mathbf{in} \; s \Rightarrow \Gamma'} \qquad \text{(T-MALLOC)}$$

$$\frac{\Theta; \Gamma, x : \tau' \vdash s_1 \Rightarrow \Gamma' \qquad \Theta; \Gamma, x : \tau \vdash s_2 \Rightarrow \Gamma'}{\Theta; \Gamma, x : \tau \vdash \mathbf{ifnull}(x) \; \mathbf{then} \; s_1 \; \mathbf{else} \; s_2 \Rightarrow \Gamma'} \qquad \text{(T-IF)}$$

$$\frac{\tau_1 + \tau_2 \approx \tau_1' + \tau_2'}{\Theta; \Gamma, x : \tau_1, y : \tau_2 \vdash \mathbf{assert}(x = y) \Rightarrow \Gamma, x : \tau_1', y : \tau_2'} \qquad \text{(T-ASSERT)}$$

$$\frac{\tau_1 + \tau_2 \approx \tau_1' + \tau_2'}{\Theta; \Gamma, x : \tau_1, y : \tau_2 \, \mathbf{ref}_f \vdash \mathbf{assert}(x = *y) \Rightarrow \Gamma, x : \tau_1', y : \tau_2' \, \mathbf{ref}_f} \qquad \text{(T-ASSERT*)}$$

$$\frac{\Theta(f) = (\tilde{\tau}) \rightarrow (\tilde{\tau}')}{\Theta; \Gamma, \tilde{x} : \tilde{\tau} \vdash f(\tilde{x}) \Rightarrow \Gamma, \tilde{x} : \tilde{\tau}'} \qquad \text{(T-CALL)}$$

$$\frac{\Gamma \approx \Gamma_1 \qquad \Gamma' \approx \Gamma_1' \qquad \Theta; \Gamma_1 \vdash s \Rightarrow \Gamma_1'}{\Theta; \Gamma \vdash s \Rightarrow \Gamma'} \qquad \text{(T-TEQ)}$$

$$\frac{\Theta; \tilde{x} : \tilde{\tau} \vdash s : \tilde{x} : \tilde{\tau}' \qquad \Theta(f) = \tilde{\tau} \rightarrow \tilde{\tau}' \; (\text{for each } f(\tilde{x}) = s \in D) \qquad dom(\Theta) = dom(D)}{\vdash D : \Theta} \qquad \text{(T-DEF)}$$

$$\frac{\vdash D : \Theta \qquad \Theta; \emptyset \vdash s \Rightarrow \emptyset}{\vdash (D, s)} \qquad \text{(T-PROG)}$$

Fig. 3. Typing Rules

Fig. 4. Snapshots of the heap during the execution of the program in Remark 2. The lefthand side and the righthand side show the states before and after executing $*y \leftarrow$ **null** respectively. The rightmost cell will be leaked.

Example 2. The following function destructively appends two lists p and q, and stores the result in $*r$.

$$\mathbf{app}(p, q, r) = \mathbf{ifnull}(p) \ \mathbf{then} \ *r \leftarrow q$$
$$\mathbf{else} \ (*r \leftarrow p; (\mathbf{let} \ x = *p \ \mathbf{in} \ \mathbf{app}(x, q, p)); \mathbf{assert}(p = *r))$$

app has type $(\tau_1, \tau_1, \top \ \mathbf{ref}_1) \rightarrow (\top, \top, \tau_1)$, where $\tau_1 = \mu\alpha.(\alpha \ \mathbf{ref}_1)$. The else-part is typed as follows.

$$\frac{\Theta; \Gamma_1 \vdash *r \leftarrow p \Rightarrow \Gamma_1 \quad \dfrac{\Theta; \Gamma_1 \vdash s \Rightarrow \Gamma_2 \quad \Theta; \Gamma_2 \vdash \mathbf{assert}(p = *r) \Rightarrow p : \top, q : \top, r : \tau_1}{\Theta; \Gamma_1 \vdash s; \mathbf{assert}(p = *r) \Rightarrow p : \top, q : \top, r : \tau_1}}{\Theta; \Gamma_1 \vdash *r \leftarrow p; s; \mathbf{assert}(p = *r) \Rightarrow p : \top, q : \top, r : \tau_1}$$

Here, $s = \mathbf{let} \ x = *p \ \mathbf{in} \ \mathbf{app}(x, q, p)$, and $\Theta, \Gamma_1, \Gamma_2$ are given by:

$$\Theta = \mathbf{app} : (\tau_1, \tau_1, \top \ \mathbf{ref}_1) \rightarrow (\top, \top, \tau_1)$$
$$\Gamma_1 = p : \tau_1, q : \tau_1, r : \top \ \mathbf{ref}_1 \qquad \Gamma_2 = p : \tau_1, q : \top, r : \top \ \mathbf{ref}_1$$

$\Theta; \Gamma_1 \vdash s \Rightarrow \Gamma_2$ is derived from:

$$\Theta; p : \top \ \mathbf{ref}_1, q : \tau_1, r : \top \ \mathbf{ref}_1, x : \tau_1 \vdash \mathbf{app}(x, q, p) \Rightarrow \Gamma_2, x : \top$$

3.3 Type Soundness

The soundness of our type system is stated as follows.

Theorem 1. *If* $\vdash (D, s)$, *then the following conditions hold.*

1. $\langle \emptyset, \emptyset, s \rangle \not\longrightarrow_D^* \mathbf{Error}$.
2. *If* $\langle \emptyset, \emptyset, s \rangle \longrightarrow_D^* \langle H, R, \mathbf{skip} \rangle$, *then* $H = \emptyset$.

The first condition means that there is no illegal read/write/free access to deallocated memory. The second condition means that well-typed programs do not leak memory.

To prove the soundness, we need to show an invariant condition that the total ownership for each (live) heap address is always 1. The invariant is expressed by the relation $\mathbf{Con}(\Gamma, H, R)$ defined below. $[\![H, v]\!]$ is the mapping from $\{0\}^*$ to the set $\mathbf{Addr}$ of addresses, defined by:

$$[\![H, v]\!](\epsilon) = v \qquad [\![H, v]\!](w0) = \begin{cases} H(h) \ \text{if} \ [\![H, v]\!](w) = h \in dom(H) \\ \mathbf{null} \ \ \text{otherwise} \end{cases}$$

9

$\mathbf{own}(H, v, \tau)(w)$ is defined by:

$$\mathbf{own}(H, v, \tau)(w) = \begin{cases} \{h \mapsto [\![\, \tau \,]\!](w)\} \text{ if } [\![\, H, v \,]\!](w) = h \neq \mathbf{null} \\ \emptyset \qquad\qquad\qquad \text{ if } v = \mathbf{null} \end{cases}$$

We write $\mathbf{ownall}(H, v, \tau)$ for $\sum_{w \in 0^*} \mathbf{own}(H, v, \tau)(w)$.

(Here, the sum of two functions $f_0 + f_1$ is defined by $\forall x \in dom(f_0) \cap dom(f_1).(f_0 + f_1)(w) = f_0(w) + f_1(w)$ and $\forall x \in dom(f_i) \setminus dom(f_{1-i}).(f_0 + f_1)(w) = f_i(w)$. $\mathbf{ownall}(H, v, \tau)(h) = \infty$ if $\sum_{w \in 0^*} \mathbf{own}(H, v, \tau)(w)(h)$ does not converge.) Intuitively, $\mathbf{ownall}(H, v, \tau)$ describes all the ownerships for the heap H, held by the value v of type τ.

A triple (Γ, H, R) is *consistent*, written $\mathbf{Con}(\Gamma, H, R)$, if the following conditions hold:

1. $dom(\Gamma) = dom(R)$
2. Let $F = \sum_{x \in dom(\Gamma)} \mathbf{.ownall}(H, R(x), \Gamma(x))$. $F(h) = 1$ for any $h \in dom(H)$ and $F(h) = 0$ for any $h \notin dom(F) \setminus dom(H)$.

We write $\mathbf{empty}_R(\Gamma)$ if $R(x) = \mathbf{null}$ or $\mathbf{empty}(\Gamma(x))$ holds for every $x \in dom(\Gamma)$. The followings are key lemmas: See Appendix C for the proofs.

Lemma 1 (lack of immediate error). *If $\Theta; \Gamma \vdash s \Rightarrow \Gamma''$ and $\vdash D : \Theta$ with $\mathbf{Con}(\Gamma, H, R)$, then $\langle H, R, s \rangle \not\longmapsto_D \mathbf{Error}$.*

Lemma 2 (lack of memory leak). *If $\mathbf{empty}_R(\Gamma)$ and $\mathbf{Con}(\Gamma, H, R)$, then $H = \emptyset$.*

Lemma 3 (type preservation). *Suppose $\Theta; \Gamma \vdash s \Rightarrow \Gamma''$ and $\vdash D : \Theta$, with $\mathbf{Con}(\Gamma, H, R)$. If $\langle H, R, s \rangle \longrightarrow_D^* \langle H', R', s' \rangle$ and $(dom(R') \setminus dom(R)) \cap dom(\Gamma) = \emptyset$, then there exist Γ' and Γ_0 such that $\Theta; \Gamma' \vdash s' \Rightarrow \Gamma'', \Gamma_0$ and $\mathbf{Con}(\Gamma', H', R')$ with $\mathbf{empty}_{R'}(\Gamma_0)$.*

We can now prove Theorem 1.

Proof of Theorem 1 Suppose $\vdash (D, s)$. Then, $\vdash D : \Theta$ and $\Theta; \emptyset \vdash s \Rightarrow \emptyset$. We have $\mathbf{Con}(\emptyset, \emptyset, \emptyset)$. To show the first property of the theorem, assume $\langle \emptyset, \emptyset, s \rangle \longrightarrow_D^* \langle H, R, s' \rangle$. By Lemma 3, we have $\Gamma_1 \vdash s' \Rightarrow \Gamma', \Gamma_0$ with $\mathbf{Con}(\Gamma_1, H, R)$. By Lemma 1, we have $\langle H, R, s' \rangle \not\longmapsto_D \mathbf{Error}$.

To show the second property of the theorem, assume that $\langle \emptyset, \emptyset, s \rangle \longrightarrow_D^* \langle H, R, \mathbf{skip} \rangle$. By Lemma 3, we have $\Gamma_1 \vdash \mathbf{skip} \Rightarrow \Gamma', \Gamma_0$ and $\mathbf{Con}(\Gamma_1, H, R)$ with $\mathbf{empty}_R(\Gamma', \Gamma_0)$ for some Γ_0 and Γ_1. By the typing rules, it must be the case that $\mathbf{empty}_R(\Gamma_1)$. By the condition $\mathbf{Con}(\Gamma_1, H, R)$ and Lemma 2, we have $H = \emptyset$ as required. $\qquad\square$

3.4 Type Inference

By Theorem 1, for verifying lack of memory-related errors in a program, it suffices to check that the program is well-typed. For the purpose of automated type

inference, we restrict the syntax of types to those of the form $(\mu\alpha.\alpha\ \mathbf{ref}_{f_1})\ \mathbf{ref}_{f_2}$. This restriction does not seem so restrictive for realistic programs: in fact, all the correct programs we have checked so far (including those given in this paper) are typable in the restricted type system.

Given a program written in our language, type inference proceeds as follows.

1. For each n-ary function f, prepare a type template

$$((\mu\alpha.\alpha\ \mathbf{ref}_{\eta_{f,1,1}})\ \mathbf{ref}_{\eta_{f,1,2}}, \ldots, (\mu\alpha.\alpha\ \mathbf{ref}_{\eta_{f,n,1}})\ \mathbf{ref}_{\eta_{f,n,2}})$$
$$\rightarrow ((\mu\alpha.\alpha\ \mathbf{ref}_{\eta'_{f,1,1}})\ \mathbf{ref}_{\eta'_{f,1,2}}, \ldots, (\mu\alpha.\alpha\ \mathbf{ref}_{\eta'_{f,n,1}})\ \mathbf{ref}_{\eta'_{f,n,2}}),$$

   where $\eta_{f,i,j}$ and $\eta'_{f,i,j}$ are variables to denote unknown ownerships. Also, for each program point p and for each variable x live at p, prepare a type template $(\mu\alpha.\alpha\ \mathbf{ref}_{\eta_{p,x,1}})\ \mathbf{ref}_{\eta_{p,x,2}}$.

2. Generate linear inequalities on ownership variables based on the typing rules and the well-formedness condition.

3. Solve the linear inequalities. If the inequalities have a solution, the program is well-typed.

The number of ownership variables and linear inequalities is quadratic in the size of the input program. Since linear inequalities (over rational numbers) can be solved in time polynomial in the size of the inequalities, the whole algorithm runs in time polynomial in the size of the input program.

Remark 3. The main advatange of using fractions in the type system given above is the exisitence of a polynomial-time algorithm for solving constraints. Fractions also increase the expressive power of the type system (compared with 0-1 ownerships). For example, consider the following program:

```
let f(x,y) = (let z=*x in let w=*y in skip) in f(p, p)
```

Our type system accepts the program above by assigning to $\mathtt{f}$ the type $(\top\ \mathbf{ref}_{0.5}, \top\ \mathbf{ref}_{0.5}) \rightarrow (\top\ \mathbf{ref}_{0.5}, \top\ \mathbf{ref}_{0.5})$. The program is not typable if we have only 0-1 ownerships (note that non-zero ownerships must be passed to x and y).

4 Extensions and Limitations

We have so far considered a very simple language which has only pointers as values. This section discusses extensions of the type system for other language features (mainly of the C language).

It is straightforward to extend the type system to handle primitive types such as integers and floating points. For structures with n elements (for the sake of simplicity, assume that each element has the same size as a pointer), we can introduce a type of the form $(\tau_0 \times \cdots \times \tau_{n-1})\ \mathbf{ref}_{w_0,\ldots,w_{n-1},f}$ as the type of a pointer to a structure. Here, τ_i is the type of the i-th element of the structure, f denotes the obligation to deallocate the structure, and w_i is a capability to read/write the i-th element; thus, an ownership has been split

```
fun delnext(p) =
  let nextp = p+1 in let next = *nextp in
  let nnp = next+1 in nn = *nnp in
     *nn <- p; *nextp <- nn; assert(nnp=next+1);
     free(next); assert(nextp=p+1);
```

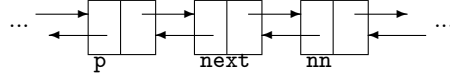**Fig. 5.** A function manipulating a doubly-linked list.

Fig. 6. A doubly-linked list given as an input of `delnext`. The cell `next` is removed and deallocated.

into a free obligation and read/write capabilities. Then the rules for pointer dereference and pointer arithmetics are given by:

$$\frac{\begin{array}{c}\Theta; \Gamma, x : \tau_{0,x}, y : (\tau_{0,y} \times \tau_1 \times \cdots \times \tau_{n-1}) \; \mathbf{ref}_{w_0,\ldots,w_{n-1},f} \vdash s \Rightarrow \Gamma', x : \tau' \\ w_0 > 0 \qquad \tau_0 \approx \tau_{0,x} + \tau_{0,y} \qquad \mathbf{empty}(\tau')\end{array}}{\Theta; \Gamma, y : (\tau_0 \times \tau_1 \times \cdots \times \tau_{n-1}) \; \mathbf{ref}_{w_0,\ldots,w_{n-1},f} \vdash \mathbf{let} \; x = *y \; \mathbf{in} \; s \Rightarrow \Gamma'}$$

$$\frac{\begin{array}{c}\Theta; \Gamma, x : (\tau_{i,x} \times \cdots \times \tau_{n-1,x}, \top, \ldots, \top) \; \mathbf{ref}_{w_{i,x},\ldots,w_{n-1,x},0,\ldots,0,0}, \\ y : (\tau_{0,y} \times \cdots \times \tau_{n-1,y}) \; \mathbf{ref}_{w_{0,y},\ldots,w_{n-1,y}}, f \vdash s \Rightarrow \Gamma', x : \tau_x \\ \forall j \in \{0, \ldots, i-1\}.(\tau_{j,y} \approx \tau_j \wedge w_j = w_{j,y}) \\ \forall j \in \{i, \ldots, n-1\}.(\tau_j \approx \tau_{j,y} + \tau_{j,x} \wedge w_j = w_{j,x} + w_{j,y}) \qquad \mathbf{empty}(\tau_x)\end{array}}{\Theta; \Gamma, y : (\tau_0 \times \cdots \times \tau_{n-1}) \; \mathbf{ref}_{w_0,\ldots,w_{n-1},f} \vdash \mathbf{let} \; x = y + i \; \mathbf{in} \; s \Rightarrow \Gamma'}$$

For example, consider the function `delnext` in Figure 5. It takes a doubly-linked list as shown in Figure 6, and deletes the next element of p. The function is given the type $(\tau_P \times \tau_N) \; \mathbf{ref}_{1,1,1} \rightarrow (\tau_P \times \tau_N) \; \mathbf{ref}_{1,1,1}$, where $\tau_P = \mu\alpha.((\alpha \times \top) \; \mathbf{ref}_{1,1,1})$ and $\tau_N = \mu\alpha.((\top \times \alpha) \; \mathbf{ref}_{1,1,1})$. The type $(\tau_P \times \tau_N) \; \mathbf{ref}_{1,1,1}$ means that the first element of `p` holds the capabilities and obligations on the cells reachable through the backward pointers, and the second element holds those on the cells reachable through the forward pointers. The types of variables at each program point are given in Appendix B.

An array of primitive values can be treated as one big reference cell, assuming that array boundary errors are prevented by other methods (such as dynamic checks or static analyses). At this moment, however, we do not know how to deal with arrays of pointers.

A dereference of a function pointer in C can be replaced with a non-deterministic choice of the functions it may point to, by using a standard flow analysis. It is not clear, however, how to deal with higher-order functions in functional languages, especially those stored in reference cells.

Cast operations can be handled in a conservative manner. For example, a pointer to a structure of type $(\tau_0 \times \cdots \times \tau_{n-1}) \; \mathbf{ref}_{w_0,\ldots,w_{n-1},f}$ can be casted to a pointer of type $(\tau_0 \times \cdots \times \tau_{m-1}) \; \mathbf{ref}_{w_0,\ldots,w_{m-1},f'}$ (if $m \leq n$). An integer can be casted to a pointer with 0 ownership (but it is useless).
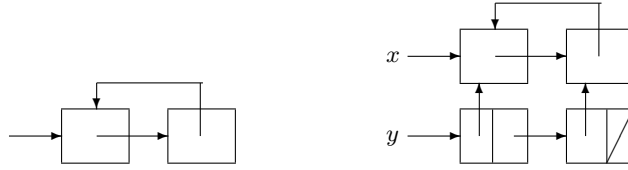
Fig. 7. Cyclic Lists

Besides arrays of pointers and higher-order functions, one of the major limitations of our type system is that it cannot deal with cyclic structures well. For example, consider a cyclic list shown on the lefthand side of Figure 7. The only type that can be assigned to cycles of an arbitrary length is $\top$: Notice that if we assign $\mu\alpha.(\alpha\ \mathbf{ref}_f)$ to the cycle, then an ownership f can be extracted for *each path* (e.g., ϵ, 00, 0000,... for the cell on the lefthand side). We have to maintain the invariant that $f + f + f + \cdots \leq 1$, so that f must be 0. Thus, although a cyclic list can be constructed, it is useless as there is no ownership. Note, however, that this limitation does not apply to the case of doubly-linked lists discussed above, since cycles in doubly-linked lists are formed by two kinds of pointers; forward and backward pointers.

If we give up detecting illegal read operations (but still prevent illegal write/free operations), then cyclic lists can be constructed and used in a restricted manner, as shown on the righthand side of Figure 7. Here, y holds the ownerships of all the cells, but x can use the cylic list in a read-only manner.

5   Experiments

We have implemented a prototype verifier for an extension of the language of Section 2 with cons cells (structures of size 2, as discussed in Section 4), and tested it for programs manipulating lists, doubly-linked lists and trees. The implementation, written in Objective Caml, is available at `http://www.kb.ecei.tohoku.ac.jp/~suenaga/mallocfree/`. As a linear programming solver, we used GLPK 4.15 wrapped by ocaml-glpk 0.1.5.

Figure 8 shows the result of the experiments. We used a machine with an Intel Core 2 1.06GHz CPU, 2MB cache and 2GB memory. The programs used for the experiments are:

- **ll-app**, **ll-reverse** and **ll-search**: create lists, perform specific operations on the lists (append for **ll-app**, reverse for **ll-reverse**, and list search for ll-search), and deallocate the lists.
- **dl-insert** and **dl-remove**: create doubly-linked lists, insert or delete a cell, and deallocating the doubly-linked lists.
- **bt-insert**: creates a binary tree, inserts a node, and then deallocates the tree.

All the programs have been verified correctly. It is worth noting that the programs manipulating doubly-linked lists could be verified. The benchmark results

13

benchmark	IC	TOTAL	GEN_LP	SOLVE_LP	NASSERT
ll-app	36	269.4	144.1	124.9	8
ll-reverse	29	139.9	70.79	68.64	4
ll-search	27	115.7	56.66	58.73	5
ll-merge	40	303.6	171.0	59.18	7
dl-insert	53	715.8	387.4	327.9	14
dl-delete	47	505.9	271.5	234.0	10
bt-insert	41	256.0	138.0	117.3	6

Fig. 8. Benchmark result. Columns IC, TOTAL, GEN_LP, SOLVE_LP and NASSERT are the number of instructions, total execution time (msec), execution time for reducing constraints into linear inequalities (msec), execution time for solving linear inequalities (msec) and the number of manually-inserted assertions.

show that our analysis is reasonably fast, despite that our current implementation is rather naive.

Limitations of the current implementation are as follows.

– Requirement for insertion of appropriate assertions. Judging from the experiments, however, an extremely simple intra-procedural analysis is sufficient for inserting the assertions automatically, except the case for doubly-linked lists, for which assertions on the structure of doubly-linked lists (like `p->next->prev = p`) are required.
– Poor error messages. Given an ill-typed program, the current system does produce some diagnostic information to indicate a possible location of a bug, but more helpful messages are needed for end-users.

6 Related Work

There are a lot of studies and tools to detect or prevent memory-related errors. They are classified into static and dynamic analyses. We focus here on static analysis techniques. In general, dynamic analysis can only detect errors that occur in particular runs.

We have already discussed Heine and Lam's work [3] in Section 1. They use polymorphism on ownerships to make the analysis context-sensitive. The same technique would be applicable to our type system. Dor, Rodeh, and Sagiv [2] use shape analysis techniques to verify lack of memory-related errors in list-manipulating programs. Unlike ours, their analysis can also detect null-pointer dereferences. Advantages of our type system over their analysis are probably efficiency and simplicity. It is not clear whether their analysis can be easily extended to handle procedure calls and data structures (e.g., trees and doubly-linked lists) other than singly-linked lists in a efficient manner. Orlovich and Rugina [4] proposed a backward dataflow analysis to detect memory leaks. Their analysis does not detect double-frees and illegal accesses to deallocated memory.

Xie and Aiken [8] use a SAT solver to detect memory leaks. Their analysis is unsound for loops and recursion.

Other potential advantages of our type-based approach are: By allowing programmers to declare ownership types, they may serve as good specifications of functions or modules, and also enhance modular verification. Our approach can be probably extended to deal with multi-threaded programs, along the line of previous work using fractional capabilities [1, 6, 7].

A main limitation of our approach is that our type system cannot handle cycles (recall the discussion in Section 4) and value-dependent (or, path-sensitive) behaviors. In practice, therefore, a combination of our technique with other techniques would be useful (e.g., shape analysis or separation logic for handling cycles, SAT-solver-based analysis [8] for handling value-dependent behaviors).

Boyland [1] is the pioneer who introduced fractions in the context of type-based program analysis. He used fractional permissions (for read/write operations) to prevent race conditions in multi-threaded programs. Terauchi [6, 7] later found another advantage of using fractions: inference of fractional permissions (or capabilities) can be reduced to a linear programming problem (rather than integer linear programming), which can be solved in polynomial time. The type system of this paper mainly exploits the latter advantage. In their work [1, 6, 7], a fractional capability is assigned to an abstract location (often called a region), while our type system assigns a fractional ownership to each access path from a variable. The former approach is not suitable for the purpose of our analysis: for example, all the elements in a list are abstracted to the same location, so that a separate ownership cannot be assigned to each element of the list.

Swamy et al. [5] developed a language with safe manual memory management. Unlike C, their language requires programmers to provide various annotations (such as whether a pointer is aliased or not).

7 Conclusion

We have proposed a new type system that guarantees lack of memory-related errors. The type system is based on the notion of fractional ownerships, and is equipped with a polynomial-time type inference algorithm. The type system is quite simple (especially compared with previous techniques for analyzing similar properties), yet it can be used to verify tricky pointer-manipulating programs.

Acknowledgment

References

1. J. Boyland. Checking interference with fractional permissions. In *Proceedings of SAS 2003*, volume 2694 of *LNCS*, pages 55–72. Springer-Verlag, 2003.

2. N. Dor, M. Rodeh, and S. Sagiv. Checking cleanness in linked lists. In *Proceedings of SAS 2000*, volume 1824 of *LNCS*, pages 115–134. Springer-Verlag, 2000.
3. D. L. Heine and M. S. Lam. A practical flow-sensitive and context-sensitive c and c++ memory leak detector. In *Proc. of PLDI*, pages 168–181, 2003.
4. M. Orlovich and R. Rugina. Memory leak analysis by contradiction. In *Proceedings of SAS 2006*, volume 4134 of *LNCS*, pages 405–424. Springer-Verlag, 2006.
5. N. Swamy, M. W. Hicks, G. Morrisett, D. Grossman, and T. Jim. Safe manual memory management in cyclone. *Sci. Comput. Program.*, 62(2):122–144, 2006.
6. T. Terauchi. Checking race freedom via linear programming. In *Proc. of PLDI*, pages 1–10, 2008.
7. T. Terauchi and A. Aiken. A capability calculus for concurrency and determinism. *ACM Trans. Prog. Lang. Syst.*, 30(5), 2008.
8. Y. Xie and A. Aiken. Context- and path-sensitive memory leak detection. In *ACM SIGSOFT International Symposium on Foundations of Software Engineering*, pages 115–125, 2005.

Appendix

A The Transition Rules Omitted in Section 2

$$\overline{\langle H, R, E[\textbf{skip}; s]\rangle \longrightarrow_D \langle H, R, E[s]\rangle}$$

$$\frac{x' \notin dom(R)}{\langle H, R, E[\textbf{let } x = \textbf{null in } s]\rangle \longrightarrow_D \langle H, R\{x' \mapsto \textbf{null}\}, E[[x'/x]s]\rangle}$$

$$\frac{R(x) \neq \textbf{null}}{\langle H, R, E[\textbf{ifnull}(x) \textbf{ then } s_1 \textbf{ else } s_2]\rangle \longrightarrow_D \langle H, R, E[s_2]\rangle}$$

$$\frac{R(x) = R(y)}{\langle H, R, E[\textbf{assert}(x = y)]\rangle \longrightarrow_D \langle H, R, E[\textbf{skip}]\rangle}$$

$$\frac{R(x) \neq R(y)}{\langle H, R, E[\textbf{assert}(x = y)]\rangle \longrightarrow_D \textbf{AssertFail}}$$

B Typing for `delnext`

For the function `delnext` discussed in Section 4, the following types are given at each program point. ($\tau_1 \times \tau_2 \, \textbf{ref}_{w_1, w_2, f}$ should be read $(\tau_1 \times \tau_2) \, \textbf{ref}_{w_1, w_2, f}$.)

```
fun delnext(p) =
  let nextp = p+1 in

  let next = *nextp in

  let nnp = next+1 in

  let nn = *nnp in

  *nn <- p;

  *nextp <- nn

  assert(nnp=next+1);

  free(next)

  assert(nextp=p+1);
```

$p : \tau_P \times \tau_N \, \textbf{ref}_{1,1,1}$

$p : \tau_P \times \top \, \textbf{ref}_{1,0,1}, \textsf{nextp} : \tau_N \times \top \, \textbf{ref}_{1,0,0}$

$p : \tau_P \times \top \, \textbf{ref}_{1,0,1}, \textsf{nextp} : \top \times \top \, \textbf{ref}_{1,0,0}, \textsf{next} : \tau_N$

$p : \tau_P \times \top \, \textbf{ref}_{1,0,1}, \textsf{nextp} : \top \times \top \, \textbf{ref}_{1,0,0},$
$\textsf{next} : \top \times \top \, \textbf{ref}_{1,0,1}, \textsf{nnp} : \tau_N \times \top \, \textbf{ref}_{1,0,0}$

$p : \tau_P \times \top \, \textbf{ref}_{1,0,1}, \textsf{nextp} : \top \times \top \, \textbf{ref}_{1,0,0},$
$\textsf{next} : \top \times \top \, \textbf{ref}_{1,0,1}, \textsf{nnp} : \top \times \top \, \textbf{ref}_{1,0,0}, \textsf{nn} : \tau_N$

$p : \tau_P \times \top \, \textbf{ref}_{1,0,1}, \textsf{nextp} : \top \times \top \, \textbf{ref}_{1,0,0},$
$\textsf{next} : \top \times \top \, \textbf{ref}_{1,0,1}, \textsf{nnp} : \top \times \top \, \textbf{ref}_{1,0,0}, \textsf{nn} : \tau_N$

$p : \tau_P \times \top \, \textbf{ref}_{1,0,1}, \textsf{nextp} : \tau_N \times \top \, \textbf{ref}_{1,0,0},$
$\textsf{next} : \top \times \top \, \textbf{ref}_{1,0,1}, \textsf{nnp} : \top \times \top \, \textbf{ref}_{1,0,0}, \textsf{nn} : \top$

$p : \tau_P \times \top \, \textbf{ref}_{1,0,1}, \textsf{nextp} : \tau_N \times \top \, \textbf{ref}_{1,0,0},$
$\textsf{next} : \top \times \top \, \textbf{ref}_{1,1,1}, \textsf{nnp} : \top \times \top \, \textbf{ref}_{0,0,0}, \textsf{nn} : \top$

$p : \tau_P \times \top \, \textbf{ref}_{1,0,1}, \textsf{nextp} : \tau_N \times \top \, \textbf{ref}_{1,0,0},$
$\textsf{next} : \top \times \top \, \textbf{ref}_{0,0,0}, \textsf{nnp} : \top \times \top \, \textbf{ref}_{0,0,0}, \textsf{nn} : \top$

$p : \tau_P \times \tau_N \, \textbf{ref}_{1,1,1}, \textsf{nextp} : \top \times \top \, \textbf{ref}_{0,0,0},$
$\textsf{next} : \top \times \top \, \textbf{ref}_{0,0,0}, \textsf{nnp} : \top \times \top \, \textbf{ref}_{0,0,0}, \textsf{nn} : \top$

17

C Proofs of Main Lemmas

Proof of Lemma 1 Suppose $\Theta; \Gamma \vdash s \Rightarrow \Gamma''$ and $\vdash D : \Theta$ with $\mathbf{Con}(\Gamma, H, R)$, but $\langle H, R, s \rangle \longrightarrow_D \mathbf{Error}$.

s must be either of the form $E[*x \leftarrow y]$, $E[\mathbf{free}(()x)]$, or $E[\mathbf{let}\ y = *x\ \mathbf{in}\ s]$, By the typing rules, it must be the case that $\Gamma(x) = \tau\ \mathbf{ref}_k$ for some τ and k such that $k > 0$. By the condition $\mathbf{Con}(\Gamma, H, R)$, it must be the case that $R(x) \in dom(H)$ or $R(x) = \mathbf{null}$, which contradicts with $\langle H, R, s \rangle \longrightarrow_D \mathbf{Error}$.

$\square$

$\square$

To prove Lemma 3, we prepare some lemmas.

We write $F_0 \approx F_1$ if $F_0(h) = F_1(h)$ for every $h \in dom(F_0) \cup dom(F_1)$ and $F_i(h) = 0$ for every $h \in dom(F_i) \setminus dom(F_{1-i})$.

Lemma 4. *Let* $F_0 = \mathbf{ownall}(H, v, \tau)$ *and* $F_1 = \mathbf{ownall}(H\{h \mapsto v'\}, v, \tau)$. *If* $F_0(h) = 0$, *then* $F_0 \approx F_1$.

Proof. It suffices to show that $F_0(w) \approx F_1(w)$ for any $w \in \{0\}^*$. If there exists a prefix w_1 of w such that $[\![H, v]\!] w_1 = h$, then let w_1' be the shortest one among such prefixes. By the condition $F_0(h) = 0$, we have $[\![\tau]\!](w_1) = 0$. By the well-formedness condition of τ, we have $[\![\tau]\!] w = 0$. Thus, by the definition of $\mathbf{own}(H, v, \tau)$, $F_0 \approx \emptyset \approx F_1$.

If there exists no prefix w_1 of w such that $[\![H, v]\!] w_1 = h$, then $F_0(w) = F_1(w)$.

Lemma 5 (weakening). *If* $\Theta; \Gamma \vdash s \Rightarrow \Gamma'$ *and* $x \notin dom(\Gamma) \cup dom(\Gamma')$, *then* $\Theta; \Gamma, x : \tau \vdash s \Rightarrow \Gamma', x : \tau$.

Proof. This follows from straightforward induction on the derivation of $\Gamma \vdash s \Rightarrow \Gamma'$. $\square$

Proof of Lemma 3 The proof proceeds by induction on the derivation of $\Gamma \vdash s \Rightarrow \Gamma''$, with case analysis on the last rule used.

– Case where the last rule is T-Skip or T-Teq: Trivial.
– Case T-Assign: In this case, we have:

$$s = *x \leftarrow y$$
$$\Gamma = \Gamma_1, x : \tau'\ \mathbf{ref}_f, y : \tau$$
$$\Gamma'' = \Gamma_1, x : \tau_1\ \mathbf{ref}_f, y : \tau_2$$
$$\tau \approx \tau_1 + \tau_2 \qquad \mathbf{empty}(\tau') \qquad f = 1$$
$$H' = H\{R(x) \mapsto R(y)\} \qquad R' = R \qquad s' = \mathbf{skip}$$

Let $\Gamma' = \Gamma''$ and $\Gamma_0 = \emptyset$. Then, we have $\Theta; \Gamma' \vdash s' \Rightarrow \Gamma', \Gamma_0$ and $\mathbf{empty}_{R'}(\Gamma_0)$. It remains to show $\mathbf{Con}(\Gamma', H', R')$. The first condition for $\mathbf{Con}(\Gamma', H', R')$ follows by $dom(\Gamma') = dom(\Gamma) = dom(R) = dom(R')$. Define F_0 and F_1 by:

$$F_0 = F_0' + \mathbf{ownall}(H, R(x), \Gamma(x)) + \mathbf{ownall}(H, R(y), \Gamma(y))$$
$$F_1 = F_1' + \mathbf{ownall}(H', R'(x), \Gamma'(x)) + \mathbf{ownall}(H', R'(y), \Gamma''(y))$$
$$F_0' = \sum_{z \in dom(\Gamma) \setminus \{R(x), R(y)\}} \mathbf{ownall}(H, R(z), \Gamma(z))$$
$$F_1' = \sum_{z \in dom(\Gamma) \setminus \{R(x), R(y)\}} \mathbf{ownall}(H', R'(z), \Gamma'(z))$$

18

It suffices to show that $F_0 \approx F_1$. Since $\mathbf{ownall}(H, R(x), \Gamma(x))(R(x)) = 1$, we have $F_0'(R(x)) = 0$. By Lemma 4, we obtain $F_0' \approx F_1'$. It remains to show

$$\mathbf{ownall}(H, R(x), \Gamma(x)) + \mathbf{ownall}(H, R(y), \Gamma(y))$$
$$\approx \mathbf{ownall}(H', R'(x), \Gamma''(x)) + \mathbf{ownall}(H', R'(y), \Gamma'(y)),$$

which is obtained as follows.

$$\mathbf{ownall}(H, R(x), \Gamma(x)) + \mathbf{ownall}(H, R(y), \Gamma(y))$$
$$\approx \{R(x) \mapsto 1\} + \mathbf{ownall}(H, R(y), \tau) \qquad (\mathbf{empty}(\tau'))$$
$$\approx \{R(x) \mapsto 1\} + \mathbf{ownall}(H, R(y), \tau_1) + \mathbf{ownall}(H, R(y), \tau_1) \quad (\tau_1 + \tau_2 \approx \tau)$$
$$\approx \mathbf{ownall}(H', R(x), \Gamma''(x)) + \mathbf{ownall}(H', R(y), \Gamma''(y))$$

The last line follows from $H'(R(x)) = R(y)$ and $\Gamma'(x) = \tau_1 \, \mathbf{ref}_1$.

– Case T-Free: In this case, we have:

$$s = \mathbf{free}(()x) \qquad s' = \mathbf{skip}$$
$$\Gamma = \Gamma_1, x : \tau \, \mathbf{ref}_1$$
$$\mathbf{empty}(\tau) \qquad \Gamma'' = \Gamma_1, x : \tau \, \mathbf{ref}_0$$
$$H' = H \setminus \{R(x)\} \qquad R' = R \qquad R(x) \in dom(H) \cup \{\mathbf{null}\}$$

Let $\Gamma' = \Gamma''$ and $\Gamma_0 = \emptyset$. Then we have $\Theta; \Gamma' \vdash s' \Rightarrow \Gamma'', \Gamma_0$.
It remains to show $\mathbf{Con}(\Gamma', H', R')$. The first condition for $\mathbf{Con}(\Gamma', H', R')$ follows by $dom(\Gamma') = dom(\Gamma) = dom(R) = dom(R')$. Define F_0 and F_1 by:

$$F_0 = F_0' + \mathbf{ownall}(H, R(x), \tau \, \mathbf{ref}_1)$$
$$F_1 = F_1' + \mathbf{ownall}(H', R'(x), \tau \, \mathbf{ref}_0)$$
$$F_0' = \sum_{z \in dom(\Gamma) \setminus \{R(x)\}} \mathbf{ownall}(H, R(z), \Gamma(z))$$
$$F_1' = \sum_{z \in dom(\Gamma) \setminus \{R(x)\}} \mathbf{ownall}(H', R'(z), \Gamma'(z))$$

If $R(x) = \mathbf{null}$, then we have $F_0 \approx F_1$ and $H' = H$, so that $\mathbf{Con}(\Gamma', H', R')$ follows immediately from $\mathbf{Con}(\Gamma, H, R)$.

Otherwise, let $h = R(x) \neq \mathbf{null}$. By the condition $\mathbf{Con}(\Gamma, H, R)$, we have $F_0(h) = 1$, which implies $F_0'(h) = 0$. By Lemma 4, we have $F_0' \approx F_1'$. Thus, $F_1 \approx F_0\{h \mapsto 0\}$, which implies $\mathbf{Con}(\Gamma', H', R')$ as required.

– Case T-Seq: In this case, we have:

$$s = s_1; s_2$$
$$s' = s_1'; s_2$$
$$\langle H, R, s_1 \rangle \longrightarrow_D \langle H', R', s_1' \rangle$$
$$\Gamma \vdash s_1 \Rightarrow \Gamma_1 \qquad \Gamma_1 \vdash s_2 \Rightarrow \Gamma''$$

By the induction hypothesis, there exist Γ' and Γ_0 such that $\Gamma' \vdash s_1' \Rightarrow \Gamma_1, \Gamma_0$ with $\mathbf{empty}_{R'}(\Gamma_0)$ and $\mathbf{Con}(\Gamma', R', H')$. By applying Lemma 5 to $\Gamma_1 \vdash s_2 \Rightarrow \Gamma''$, we obtain $\Gamma_1, \Gamma_0 \vdash s_2 \Rightarrow \Gamma'', \Gamma_0$. By using T-Seq, we obtain $\Gamma' \vdash s' \Rightarrow \Gamma'', \Gamma_0$ as required.

– Case T-NULL: In this case, we have:

$$s = \textbf{let } x = \textbf{null in } s_1$$
$$s' = [x'/x]s_1$$
$$H' = H \qquad R' = R\{x' \mapsto \textbf{null}\}$$
$$\Theta; \Gamma, x : \tau \vdash s_1 \Rightarrow \Gamma'', x : \tau'$$

Let $\Gamma' = \Gamma, x' : \tau$ and $\Gamma_0 = x' : \tau'$. Then, we have $\Gamma' \vdash s' \Rightarrow \Gamma'', \Gamma_0$ and $\textbf{empty}_{R'}(\Gamma_0)$ as required.

It remains to show $\textbf{Con}(\Gamma', H', R')$. The first condition for $\textbf{Con}(\Gamma', H', R')$ follows by $dom(\Gamma') = dom(\Gamma) \cup \{x'\} = dom(R) \cup \{x\} = dom(R')$. The second condition follows from:

$$\sum_{z \in dom(\Gamma')} \textbf{ownall}(H', R'(z), \Gamma'(z))$$
$$= \sum_{z \in dom(\Gamma)} \textbf{ownall}(H, R(z), \Gamma(z)) + \textbf{ownall}(H, \textbf{null}, \tau)$$
$$= \sum_{z \in dom(\Gamma)} \textbf{ownall}(H, R(z), \Gamma(z))$$

– Case T-LET*: In this case, we have:

$$s = \textbf{let } x = *y \textbf{ in } s_1$$
$$s' = [x'/x]s_1$$
$$H' = H \qquad R' = R\{x' \mapsto H(R(y))\}$$
$$\Gamma = \Gamma_1, y : \tau \textbf{ ref}_f$$
$$\Gamma, x : \tau_1, y : \tau_2 \textbf{ ref}_f \vdash s_1 \Rightarrow \Gamma'', x : \tau_1'$$
$$\tau \approx \tau_1 + \tau_2 \qquad \textbf{empty}(\tau_1') \qquad f > 0$$

Let $\Gamma' = \Gamma, x' : \tau_1, y : \tau_2 \textbf{ ref}_f$ and $\Gamma_0 = x' : \tau_1'$. Then, we have $\Theta; \Gamma' \vdash s' \Rightarrow \Gamma'', \Gamma_0$ and $\textbf{empty}_{R'}(\Gamma_0)$. (Note that x' is a fresh variable, so that we can obtain a derivation for $\Gamma, x' : \tau_1, y : \tau_2 \textbf{ ref}_f \vdash [x'/x]s_1 \Rightarrow \Gamma'', x' : \tau_1'$ by just renaming x in $\Gamma, x : \tau_1, y : \tau_2 \textbf{ ref}_f \vdash s_1 \Rightarrow \Gamma'', x : \tau_1'$ with x'.)

It remains to show $\textbf{Con}(\Gamma', H', R')$. The first condition for $\textbf{Con}(\Gamma', H', R')$ follows by $dom(\Gamma') = dom(\Gamma) \cup \{x'\} = dom(R) \cup \{x\} = dom(R')$.

For the second condition, it suffices to show that $F_0 \approx F_1$ holds for the following F_0 and F_1.

$$F_0 = F_0' + \textbf{ownall}(H, R(y), \Gamma(y))$$
$$F_1 = F_1' + \textbf{ownall}(H', R'(y), \Gamma'(y)) + \textbf{ownall}(H', R'(x'), \Gamma'(x'))$$
$$F_0' = \sum_{z \in dom(\Gamma) \backslash \{R(y)\}} \textbf{ownall}(H, R(z), \Gamma(z))$$
$$F_1' = \sum_{z \in dom(\Gamma') \backslash \{R(y), R(x')\}} \textbf{ownall}(H', R'(z), \Gamma'(z))$$

We have $F_0 \approx F_1$ as required, since $F_0' \approx F_1'$ holds and:

$$\textbf{ownall}(H, R(y), \Gamma(y))$$
$$\approx \textbf{ownall}(H', R'(y), \Gamma'(y)) + \textbf{ownall}(H', R'(x'), \Gamma'(x')),$$

follows from $\tau \approx \tau_1 + \tau_2$.

– Case T-LET: Similar to the case for T-LET*

– Case T-Malloc: In this case, we have:

$$s = \textbf{let } x = \textbf{malloc}() \textbf{ in } s_1$$
$$s' = [x'/x]s_1$$
$$H' = H\{h \mapsto v\} \qquad h \notin dom(H) \qquad R' = R\{x' \mapsto h\} \qquad x' \notin dom(R)$$
$$\Theta; \Gamma, x : \tau \textbf{ ref}_1 \vdash s_1 \Rightarrow \Gamma'', x : \tau' \textbf{ ref}_0 \qquad \textbf{empty}(\tau) \qquad \textbf{empty}(\tau')$$

Let $\Gamma' = \Gamma, x' : \tau \textbf{ ref}_1$ and $\Gamma_0 = x' : \tau' \textbf{ ref}_0$. Then, we have $\Theta; \Gamma' \vdash s' \Rightarrow \Gamma'', \Gamma_0$ and $\textbf{empty}_{R'}(\Gamma_0)$.

It remains to show $\textbf{Con}(\Gamma', H', R')$. The first condition for $\textbf{Con}(\Gamma', H', R')$ follows from $dom(\Gamma') = dom(\Gamma) \cup \{x'\} = dom(R) \cup \{x'\} = dom(R')$.
The second condition for $\textbf{Con}(\Gamma', H', R')$ follows from

$$\sum_{z \in dom(\Gamma')} \textbf{ownall}(H', R'(z), \Gamma'(z))$$
$$= (\sum_{z \in dom(\Gamma)} \textbf{ownall}(H', R'(z), \Gamma'(z))) + \textbf{ownall}(H', h, \tau \textbf{ ref}_1)$$
$$= (\sum_{z \in dom(\Gamma)} \textbf{ownall}(H, R(z), \Gamma(z))) + \{h \mapsto 1\}$$

and $\textbf{Con}(\Gamma, H, R)$.

– Case T-If: In this case, s must be of the form $s = \textbf{ifnull}(x) \textbf{ then } s_1 \textbf{ else } s_2$. We show only the case for $R(x) = \textbf{null}$; the case for $R(x) \neq \textbf{null}$ is similar. If $R(x) = \textbf{null}$, we have:

$$s = \textbf{ifnull}(x) \textbf{ then } s_1 \textbf{ else } s_2$$
$$s' = s_1 \qquad H' = H \qquad R' = R$$
$$\Gamma = \Gamma_1, x : \tau$$
$$\Theta; \Gamma_1, x : \tau' \vdash s_1 \Rightarrow \Gamma'$$

Let $\Gamma' = \Gamma_1, x : \tau'$ and $\Gamma_0 = \emptyset$. Then, $\Theta; \Gamma' \vdash s' \Rightarrow \Gamma'', \Gamma_0$.
It remains to show $\textbf{Con}(\Gamma', H', R')$. The first condition for $\textbf{Con}(\Gamma', H', R')$ follows immediately. The second condition follows from $\textbf{ownall}(H, \textbf{null}, \Gamma(x)) = \textbf{ownall}(H, \textbf{null}, \Gamma'(x))$.

– Case T-Assert*: In this case, we have:

$$s = \textbf{assert}(x = *y)$$
$$s' = \textbf{skip}$$
$$H' = H \qquad R' = R \qquad R(x) = H(R(y))$$
$$\Gamma = \Gamma_1, x : \tau_1, y : \tau_2 \textbf{ ref}_f$$
$$\Gamma'' = \Gamma_1, x : \tau_1', y : \tau_2' \textbf{ ref}_f$$
$$\tau_1 + \tau_2 \approx \tau_1' + \tau_2'$$

Let $\Gamma' = \Gamma''$ and $\Gamma_0 = \emptyset$. Then, $\Theta; \Gamma' \vdash s' \Rightarrow \Gamma'', \Gamma_0$.
It remains to show $\textbf{Con}(\Gamma', H', R')$. The first condition for $\textbf{Con}(\Gamma', H', R')$ follows immediately.
For the second condition, it suffices to check that

$$\textbf{ownall}(H, R(y), \tau_2 \textbf{ ref}_f) + \textbf{ownall}(H, R(x), \tau_1)$$
$$\approx \textbf{ownall}(H, R(y), \tau_2' \textbf{ ref}_f) + \textbf{ownall}(H, R(x), \tau_1'),$$

which follows immediately from the conditions $\tau_1 + \tau_2 \approx \tau_1' + \tau_2'$ and $H(R(y)) = R(x)$.

- Case T-Assert: Similar to the case for T-Assert*
- Case T-Call: In this case, we have:

$$s = f(\tilde{y})$$
$$s' = [\tilde{y}/\tilde{x}]s_1$$
$$H' = H \qquad R' = R$$
$$f(\tilde{x}) = s_1 \in D$$
$$\Gamma = \Gamma_1, \tilde{y} : \tilde{\tau}$$
$$\Gamma'' = \Gamma_1, \tilde{y} : \tilde{\tau}'$$
$$\Theta; \tilde{x} : \tilde{\tau} \vdash s_1 \Rightarrow \tilde{x} : \tilde{\tau}'$$

Let $\Gamma' = \Gamma''$ and $\Gamma_0 = \emptyset$. By renaming $\tilde{x}$ with $\tilde{y}$, we get $\Theta; \tilde{y} : \tilde{\tau} \vdash s' \Rightarrow \tilde{y} : \tilde{\tau}'$ from $\Theta; \tilde{x} : \tilde{\tau} \vdash s_1 \Rightarrow \tilde{x} : \tilde{\tau}'$. By applying Lemma 5, we obtain $\Theta; \Gamma' \vdash s' \Rightarrow \Gamma'', \Gamma_0$.

$\mathbf{Con}(\Gamma', H', R')$ follows immediately from $\mathbf{Con}(\Gamma, H, R)$ (note that $\Gamma' = \Gamma$, $H' = H$, and $R' = R$.)

$\square$