Monotonic References for Gradual Typing

Jeremy G. Siek  Michael M. Vitousek
Matteo Cimini  Sam Tobin-Hochstadt
Indiana University Bloomington
jsiek@indiana.edu

Ronald Garcia
University of British Columbia
rxg@cs.ubc.ca

Abstract
Gradual typing enables both static and dynamic typing in the same program, and makes it convenient to migrate code between the two typing disciplines. We have had a satisfactory static semantics for gradual typing for some time but the dynamic semantics has proved much more difficult, raising numerous research challenges. Ongoing efforts to integrate gradual typing into existing functional and object-oriented languages revealed problems regarding space efficiency, run-time overhead, and object identity. While the first problem has been solved, the later two problems remain open. The essence of these problems is best studied in the context of the gradually-typed lambda calculus with mutable references.

In this paper we present a new dynamic semantics called monotonic references, which does not require proxies, thereby solving the object identity problem, and is the first to completely eliminate the run-time overhead associated with dynamic typing in the statically typed regions of code while maintaining the flexibility of the gradual type system. With our design, casting a reference may cause a heap cell to become less dynamically typed (but not more). However, retaining type safety is challenging in a semantics such as this that allows strong updates to the heap. Nevertheless, we have a mechanized proof that monotonic references are type safe. We present a blame tracking strategy for monotonic references and prove the blame-subtyping theorem.

Categories and Subject Descriptors D.3.1 [Programming Languages]: Formal Definitions and Theory; F.3.3 [Logics and Meanings of Programs]: Studies of Program Constructs – Type structure

General Terms Languages, Theory

Keywords  gradual typing, mutable references

1. Introduction
Static and dynamic type systems have well-known strengths and weaknesses. Static type systems provide a machine-checked form of documentation, catch bugs early, and help the compiler generate efficient code. Dynamic type systems provide the flexibility often needed during prototyping and enable powerful features such as reflection. Over the years, many languages have blurred the boundary between static and dynamic typing, such as type hints in Lisp (Steele 1990) and the addition of a dynamic type, named Dyn, to otherwise statically typed languages (Abadi et al. 1989). But the seamless and fine-grained integration of static and dynamic typing remained problematic (Thatte 1990; Oliart 1994) until Siek and Taha (2006, 2007) designed a solution named gradual typing that enables implicit casts to and from the unknown type * (aka. the dynamic type) while still catching static type errors.

The static semantics of gradual typing has worked well and seen considerable uptake in industry, including Google’s Dart language (Bracha 2011), Microsoft’s TypeScript (Heijlsberg 2012), and Facebook’s variant of PHP (Verlaguet 2013). The run-time checking aspect of gradual typing, which governs the passing of values between static and dynamic regions of a program, has met several challenges and is an ongoing area of research.

The first challenge was defining an appropriate notion of type safety for gradual typing, which was solved by Tobin-Hochstadt and Felleisen (2006) in the context of designing a coarse-grained gradual type system for Scheme (Tobin-Hochstadt and Felleisen 2008), using the notion of blame from Findler and Felleisen (2002). Wadler and Findler (2009) adapted this solution to fine-grained gradual typing in the form of the blame theorem. The second challenge was that function proxies used to implement higher-order casts can take space proportional to execution time. Herman et al. (2007, 2010) solved this problem in theory by representing casts with the coercions of Henglein (1994). Siek and Wadler (2010) developed an implementation approach for space-efficient casts.

During the development of the Thorn language (Bloom et al. 2009), Wrigstad et al. (2010) observed that the standard approach to gradually-typed mutable references, due to Herman and Flanagan (2007), incurs run-time overhead in statically-typed code. To address this problem, they introduce a distinction between like types and concrete types. Concrete types are the usual types of a statically-typed language and incur zero run-time overhead, but dynamically-typed values cannot flow into concrete types. Like types, on the other hand, provide static checking but incur run-time overhead and may refer to dynamically-typed values.

Vitousek et al. (2012, 2014) observed that the standard approach gradually-typed mutable references requires proxies and proxies cause well-known problems with object identity (Van Cutsem and Miller 2010). In fact, Vitousek et al. (2014) found that adding type annotations to existing Python programs would sometimes cause incorrect program behavior.

In this paper we investigate the essence of the run-time overhead and object-identity problems in the context of the gradually-typed lambda calculus with mutable references. We propose a new dynamic semantics, monotonic references, that does not use proxies and incurs zero overhead in statically typed code, that is, it is free
Monotonic References for Gradual Typing

1. We define the dynamic semantics for monotonic references, the first system to simultaneously solve the object-identity and run-time overhead problems while maintaining the expressiveness of gradual type systems (Sections 3 and 5).

2. We mechanize a proof of type safety in Isabelle (Section 4).

3. We augment monotonic references with blame tracking and prove the blame-subtyping theorem (Section 6). The supplemental material includes an interpreter with blame tracking.

We review the gradually-typed lambda calculus with references in Section 2 and discuss the problems of object identity and run-time overhead. We address an implementation concern regarding strong updates in Section 7 and we discuss related work in Section 8. The paper concludes in Section 9.

2. Background and Problem Statement

Figure 3 reviews the syntax and static semantics of the gradually-typed lambda calculus with references. The primary difference between gradual typing and simple typing is that uses of type equality are replaced by \textit{consistency}, also defined in Figure 3. The consistency relation enables implicit casts to and from \texttt{*}. (In contrast, an object-oriented language would only allow implicit casts to the top \texttt{Object} type.) The consistency relation is a congruence, even for reference types (Herman et al. 2010), which differs from the original treatment of references as invariant (Sieh and Taha 2006). The more flexible treatment of references enables the passing of error in such situations (see Section 2.3). On the whole, we believe monotonic references are the right design choice in scenarios where high-performance is a priority and where programmers intend to eventually convert their programs to be statically typed. Monotonic references are no more restrictive than those of statically-typed languages such as ML.

The dynamic semantics of monotonic references is particularly subtle because references may point to values that themselves contain references, and furthermore, the dynamic points-to graph may be cyclic. Thus, applying a cast to a reference requires what amounts to a fixed-point computation on a sub-region of the heap. Also, because we change heap values to have different types, that is, we perform \textit{strong updates}, it is non-trivial to prove type safety. Nevertheless, we have a mechanized proof of type safety.

In gradually-typed languages with higher-order features such as first-class functions and objects, blame tracking plays an important role in providing meaningful error messages when casts fail and it enables fine-grained guarantees, via a blame theorem, regarding which regions of the code are statically type safe. In this paper we present blame tracking for monotonic references and prove the blame-subtyping theorem. Designing blame tracking for monotonic references was a multi-year effort involving the exploration of several alternatives. The key to our design is to use the labeled types of Siek and Wadler (2010) as run-time type information (RTTI), together with three new operations on labeled types: a bidirectional cast operator that captures the dual read/write nature of mutable references, a merge operator that models how casts on separate aliases to the same heap cell interact over time, and an operator that casts heap cells from one labeled type to another.

To summarize, this paper presents a new dynamic semantics for gradually-typed mutable references that finally delivers efficiency for the statically-typed parts of a program, maintains type soundness, provides blame tracking, and relieves the problems with object identity. This result may improve the design and implementation of gradual typing for functional languages such as Racket and Clojure as well as object-oriented languages such as TypeScript, Python, and PHP. More concretely, this paper makes the following three technical contributions:

1. We define the dynamic semantics for monotonic references, the first system to simultaneously solve the object-identity and run-time overhead problems while maintaining the expressiveness of gradual type systems (Sections 3 and 5).

2. We mechanize a proof of type safety in Isabelle (Section 4).

3. We augment monotonic references with blame tracking and prove the blame-subtyping theorem (Section 6). The supplemental material includes an interpreter with blame tracking.

We review the gradually-typed lambda calculus with references in Section 2 and discuss the problems of object identity and run-time overhead. We address an implementation concern regarding strong updates in Section 7 and we discuss related work in Section 8. The paper concludes in Section 9.
Syntax

Labels \( \ell \)

Operators \( op ::= \) plus | minus | is | \( \cdots \)

Expressions \( e ::= k \mid op(\ell)(e) \mid x \mid \lambda x:T, e \mid (e \; e') \mid e \; as^\ell T \mid (e, e) \mid \text{fat } e \mid \text{and } e \mid \text{ref } e \mid ! \ell e \mid e =^\ell e \)

Consistency

\[ T \sim T \]

\[ \begin{array}{ccc}
   \times & T & T \\
   T & \sim & \star \\
   B & \sim & B \\
   \text{Ref } T_1 & \sim & \text{Ref } T_2 \\
   \end{array} \]

Expression typing

\[ \begin{array}{l}
   k : B \quad \Gamma \vdash \ell e : T \\
   \Gamma \vdash : B \quad \Gamma \vdash \ell B \rightarrow B \\
   \Gamma \vdash x : T \quad \Gamma \vdash \lambda x : T_1, e : T_2 \\
   \Gamma \vdash e_1 : T_1 \quad \Gamma \vdash e_2 : T_2 \\
   \Gamma \vdash \text{pair}(T_1, T_2) \\
   \Gamma \vdash e \rightarrow T \\
   \Gamma \vdash e \rightarrow T'' \\
   \end{array} \]

Type matching

\[ \begin{array}{l}
   \text{fun}(T_1 \rightarrow T_2, T_11, T_12) \\
   \text{pair}(T_1 \times T_2, T_11, T_12) \\
   \text{ref}(\text{Ref } T, T) \\
   \end{array} \]

Figure 3. Gradually-typed \( \lambda \) calculus with mutable references

Figure 4. Compile casts to coercions

\[ \begin{array}{l}
   (B \Rightarrow^\ell B) = \ell \\
   (I \Rightarrow^\ell I) = I! \\
   (\ast \Rightarrow^\ell \ast) = \ast \\
   (\ast \Rightarrow^\ell I) = I^\ell \\
   (T_1 \Rightarrow^\ell T_2) = (T_1^\ell \Rightarrow^\ell T_2) \\
   \end{array} \]

\[ \begin{array}{l}
   (T_1 \times T_2) = (T_1^\ell \times T_2^\ell) = (T_1 \Rightarrow^\ell T_1') \times (T_2 \Rightarrow^\ell T_2') \\
   \text{Ref } T \Rightarrow^\ell \text{Ref } T' = \text{Ref } (T \Rightarrow^\ell T')(T' \Rightarrow^\ell T) \\
   \end{array} \]

2.1 The problem with object identity

Consider the following \( \text{move} \) function that transfers an integer from one heap cell to another and zeroes out the source cell. The function starts by checking whether reference \( x \) and \( y \) are aliased using the \( \text{is} \) operator, in which case it does nothing. After the definition of \( \text{move} \), we allocate a single cell, storing the address in reference \( r \), and call \( \text{move} \) with two occurrences of \( r \).

\[
\begin{align*}
\text{let } \text{move} = &\quad \lambda x : \text{Ref Int}. \lambda y : \text{Ref Int}. \\
&\quad \text{if is}(x, y) \text{ then } () \\
&\quad \text{else } x := 0; y := 0; () \text{ in } \\
\text{let } r = \text{ref 42 in } \\
&\quad ((\text{move } r) \Rightarrow^{\ell} r) \Rightarrow^{\ell} r \\
\end{align*}
\]

The result of the above program is 42. Next suppose that we change the fourth line so that the reference \( r \) is passed through some dynamically-typed code, which we model by casting it to \( \text{Ref } \).

\[
\begin{align*}
\text{let } r = \text{ref 42} \Rightarrow^{\ell} \text{Ref } r \Rightarrow^{\ell} r & \text{ in } \\
\end{align*}
\]

The cast from \( \text{Ref Int} \) to \( \text{Ref } \) compiles to \( \text{Ref Int}^{\ell} \). The first coercion \( \text{Int}! \), an injection, is applied when reading from the reference, casting from \( \text{Int} \) to \( \ast \), and the second coercion \( \text{Int}^{\ell} \), a projection, is applied when writing to the reference, casting from \( \ast \) to \( \text{Int} \). Applying the reference coercion to the address \( a \) produced by \( \text{ref 42} \) produces \( v_1 = a(\text{Ref Int}^{\ell} \text{ Int}) \), that is, a proxied reference. There are also implicit casts in the call to \( \text{move} \), from \( \text{Ref } \) to \( \text{Ref Int} \). Each parameter is wrapped in a cast, producing \( v_2 = v_1(\text{Ref Int}^{\ell} \text{ Int}) \) and \( v_3 = v_1(\text{Ref Int}^{\ell} \text{ Int}) \). Proceeding to the body of \( \text{move} \), we come to the interesting question: what should \( \text{is}(v_2, v_3) \) return?

The \( \text{is} \) operator could compare the underlying addresses. However, it is desirable to only have \( \text{is} \) return true when the two references are behaviorally equivalent. But differently-wrapped addresses may have different behavior, for example, one may trigger an error when the other does not. Another option is for \( \text{is} \) to compare the addresses and the coercions, that is, adopt the \text{membrane}
### Syntax

Expressions: $e ::= k \mid \text{op}(\vec{c}) \mid x \mid \lambda x. e \mid e_1 e_2 \mid (e_1, e_2) \mid \text{snd}(e) \mid \text{fst}(e) \mid \text{let}(e) \mid\text{Ref}(e) \mid\text{ERef}(e) \mid\text{contract}(e) \mid(e_1, e_2, \ldots, e_n)$

Injectives: $I ::= B \mid T \rightarrow T \mid T \times T \mid \text{Ref} T$

Coercions: $c ::= \iota \mid T_1^T \mid T_1 \mid c \rightarrow e \mid e \times c \mid c ; c \mid \text{Ref} c \mid \text{ERef} c$

Values: $v ::= k \mid \lambda x. e \mid (v, v') \mid v'(!) \mid a \mid v(\text{Ref} c)$

Heap: $\mu ::= \emptyset \mid (\mu(a \rightarrow v))$

Heap Typing: $\Sigma ::= \emptyset \mid \Sigma(a \rightarrow T)$

### Expression typing

### Heap typing

### Values

### Coercion typing

#### Cast reduction rules

#### Reference reduction rules

#### State reduction rules

#### Solution of Van Cutsem and Miller (2010). However, this approach would cause in $(v_2, v_3)$ to return false, changing the result of the above program from 42 to 0. The problem is that membranes preserve identity within a single membrane but not across different membranes, which in this setting are just different casts. Alternatively, if proxies had addresses, one could compare their addresses. But that also changes the result to 0. In short, these approaches break a fundamental property of casts: adding casts to a program should not change the behavior other than to induce more cast errors. In this paper we investigate a design that does not use proxies.

#### 2.2 Run-time overhead in fully-static code

Consider the following fully-static function $f$ that dereferences its parameter $x$.

```racket
(lst f = \lambda x: \text{Ref Int}. \ i^2 (x) \in f (\text{ref} 4);  
(f (\text{ref} (\text{true as} x \rightarrow *) \ as) c \text{Ref Int})
```

In the first call to $f$, a normal reference to an integer flows into the dereference of $x$ whereas in the second call, a proxied reference flows into the dereference of $x$ (under the standard semantics). The code generated for the dereference in the body of $f$ needs to be general enough to handle both kinds of references. The code must inspect the value and dispatch, thereby incurring run-time overhead. The overhead can also be seen in the dynamic semantics (Figure 5), where there are two reduction rules for dereferencing: (DEREF) and (DEREFCAST), and two reduction rules for updating references: (UPDATE) and (UPDATECAST). Another way to look at this problem is that there are two canonical forms of type $\text{Ref Int}$, a plain address $a$ and also a value wrapped in a reference coercion, $v(\text{Ref} c_1 c_2)$. To get rid of the overhead we need a design with only a single canonical form for values of reference type.

The run-time overhead for references affects every read and write to the heap and is particularly detrimental in tight loops over arrays. When adding support for contracts to mutable data structures in Racket, Strickland et al. (2012, Figure 9) measured this overhead at approximately 25% for fully-typed code on a bubble-sort microbenchmark.

#### 2.3 Non-determinism in multi-threaded code

The standard semantics for mutable references originally proposed by Herman et al. (2010) produces an error only if type inconsistency is witnessed by some read or write to the reference, so in a non-deterministic multi-threaded program, whether a check will fail at runtime is difficult to predict.

The contract system in Racket currently implements the standard semantics (Flatt and PLT 2014). For example, the following Racket program sometimes fails and blames $b_1$, sometimes fails and blames $b_2$, and sometimes succeeds, as explained below.

```racket
#lang racket
(define b (box #f))
(define/contract b1 (box/c integer?) b)
(define/contract b2 (box/c string?) b)

(thread (lambda ()
  (for ([i [1 2]])
    (set-box! b1 5)
    (sleep 0.000000001)
    (add1 (unbox b1))))))

(thread lambda ()
  (for ([i [1 2]])
    (set-box! b2 "hello")
    (sleep 0.000000001)
    (string-append "world" (unbox b2))))
```
The program creates a single reference cell \( b \), and accesses it through two distinct proxies, \( b1 \) and \( b2 \), each with its own dynamic check. When the two threads do not interleave, the program succeeds, but if the second thread changes \( b2 \) to contain a string between the set–box! and unbox calls for \( b1 \), the system halts, blaming one of the parties.

In contrast, if \( \text{box/c} \) implemented monotonic references, then an error would deterministically occur when \( \text{define/contract} \) is used for the second time.

### 3. Monotonic References Without Blame

Figure 6 defines the syntax and semantics of our new coercion calculus with monotonic references, but without blame. Figure 8 defines the compilation of casts to monotonic coercions, also without blame. The addition of blame adds considerable complexity, so we postpone its treatment to Section 5. Typical of gradually-typed languages, there is a value form for values that have been boxed and injected to \(*\), which is \( v(!) \). The \( I \) plays the role of a tag that records the type of \( v \). The values at all other types are unboxed; the same as they would be in a statically-typed language.

With monotonic references, there is only one kind of value at reference type: normal addresses. When a cast is applied to a reference, instead of wrapping the reference with a cast, we cast the underlying value on the heap. To make sure that the new type of the value is consistent with all the outstanding references, we require that a cast only make the type of the value less dynamic (Figure 1). Otherwise the cast results in a runtime error. Thus, we maintain the heap invariant that the type of every reference in the program is at least as dynamic as the type of the value on the heap that it points to, as captured in the typing rule (WTREF).

The syntax of the monotonic calculus differs from the standard calculus with references in that there are two kinds of dereference and update expressions. Programmers need not worry about choosing which of the two dereference or update expressions to use because this choice is type directed and therefore is handled during compilation from the source language to the coercion calculus. We reserve the forms \( \ell ! e \) and \( e1 := e2 \) for situations in which the reference type is fully static (Figure 2 and expression typing in Figure 6). In these situations we know that the value in the heap has the same type as the reference thanks to Proposition 2 and our heap invariant. Thus, if a reference has a fully static type, such as \( \text{Ref Int} \), the corresponding value on the heap must be an actual integer (and not an injection to \( * \)), so we need only one reduction rule for dereferencing a fully-static reference (DEREFM), and one rule for updating a fully-static reference (UPDMD). For expressions of reference type that are not fully-static, we introduce the syntactic forms \( \ell ! e \) and \( e1 := e2 \) for dereference and update, respectively. The type annotation \( T \) records the compile-time type of \( e \), that is, \( e \) has type \( \text{Ref T} \). For example, \( T \) could be \( * \), \( * * * * \), or \( * \times \text{Int} \). Because the value on the heap might be less dynamic than \( T \), a cast is needed to mediate between \( T \) and the run-time type of the heap cell.

The reduction rule (DYNDEREFM) casts from the addresses’ run-time type, which we store next to the heap cell, to the compile-time type \( T \). We write \( \mu(a)_{\text{ref}} \) for the run-time type information for reference \( a \) and we write \( \mu(a)_{\text{val}} \) for the value in the heap cell. The reduction rule (DYNUPDMD) casts the to-be-written value \( v \) from \( T \) to the address’s run-time type, so the new contents of the cell is \( cv = v(T \Rightarrow \mu(a)_{\text{ref}}) \). This \( cv \) is not a value yet, so storing it in the heap is unusual. In earlier versions of the semantics we tried to reduce \( cv \) to a value before storing it in the heap, but there are complications that force this design, which we discuss later in this section. To summarize our treatment of dereference and update, we present efficient semantics for the fully-static dereference and update but have slightly increased the overhead for dynamic dereferences and updates. This is a price we are willing to pay to have dynamic typing “pay its own way”.

The crux of the monotonic semantics is in the reduction rules that apply a reference coercion to an address: \( \text{CASTREF1} \), \( \text{CASTREF2} \), and \( \text{CASTREF3} \). In \( \text{CASTREF1} \) we have an address that maps to \( cv \) of type \( T \) and we cast \( cv \) so that it is less or equally dynamic than both the target type \( T2 \) and all of the existing references to the cell. To accomplish this, we take the greatest lower bound of \( T3 = T1 \cap T2 \) (Figure 7) to be the new type of the cell, so the new contents is \( cv' = cv(T1 \Rightarrow T3) \). There are two side conditions on \( \text{CASTREF1} \): \( T1 \cap T2 \) must be defined and \( T3 \neq T1 \). If \( T1 \cap T2 \) is undefined, or equivalently, if \( T1 \not< T2 \), we instead signal an error, as handled by \( \text{CASTREF3} \). If \( T3 = T1 \), then there is no need to cast \( cv \), which is handled by \( \text{CASTREF2} \).

The rest of the coercion reduction rules are captured by the rule \( \text{PURECAST} \), so they are the same as in the standard semantics (Figure 5), though here we ignore blame, i.e., replace \( \text{blame} \) with \( \text{error} \). \( I2 \), with \( I2 ' \), and \( I1 \Rightarrow I2 \).

The meet function defined in Figure 7 indeed computes the greatest lower bound with respect to the less-dynamic relation.

**Proposition 3** (Meet computes the greatest lower bound).

1. \( (T1 \cap T2) \subseteq T1 \) and \( (T1 \cap T2) \subseteq T2 \).
2. If \( T \subseteq T1 \) and \( T \subseteq T2 \), then \( T \subseteq T1 \cap T2 \).

To motivate our organization of the heap, we present two examples that demonstrate why we store run-time type information and casted values, not just values, on the heap.

**Cycles and termination** The first complication is that there can be cycles in the heap and we need to make sure that when we apply a cast to an address in a cycle, the cast terminates. Consider the following example in which we create a pair whose second element is a reference back to itself.

\[
\text{let } r1 = \text{ref } (42, 0 \ast *) \text{ in } \\
\text{let } r2 = r1 \text{ as Ref } (\text{Int } \times \text{Ref } *) \text{ in } \\
\text{fast } ! r2
\]

Once the cycle is established, we cast \( r1 \) from type \( \text{Ref } (\text{Int } \times *) \) to \( \text{Ref } (\text{Int } \times \text{Ref } *) \). The presence of the nested \( \text{Ref } * \) in the target type means that the cast on \( r1 \) will trigger another cast on \( r1 \). The correct result of this program is 42 but a naive dynamic semantics would diverge. Our semantics avoids divergence by checking whether the new run-time type is equal to the old run-time type; in such cases the heap cell is left unchanged (see rule (CASTREF2)).

**Casted values in the heap** Consider the following example in which we create a triple of type \( * * * * * * \) whose third element is a reference back to itself.

\[
\text{let } r0 = \text{ref } (42 \ast *, 7 \ast *, 0 \ast *) \text{ in } \\
r0 = (42 \ast *, 7 \ast *, r0 \ast *) \text{ in } \\
\text{let } r1 = r0 \text{ as Ref } (\text{Int } \times \ast \ast \text{Ref } (\text{Int } \times \text{Int } \times *)) \text{ in } \\
\text{fast } (\text{fast } ! r1)
\]

Suppose \( a0 \) is the address created in the allocation on the first line. On line three we cast \( a0 \) in such a way that we trigger two casts on \( a0 \). Consider the action of these casts on just the first two elements of the triple, we have:

\[
* * \ast \Rightarrow \text{Int } \times \ast \ast \Rightarrow \text{Int } \times \text{Int}
\]

The second cast occurs while the first is still in progress. Now, suppose we delayed updating the heap cell until we finished reducing to a value. At the moment when we apply the second cast, we would still have the original value, of type \( * * * * \), in the heap. This is problematic because our next step would be to apply a cast from \( \text{Int } \times \ast \Rightarrow \text{Int } \times \text{Int} \) to this value, but the value’s type and the
Expressions  
\[ e ::= \ldots | \text{ref} \, T \, e \mid \text{te} @ T \mid e := e @ T \mid \text{error} \]

Coercions  
\[ c ::= \ldots \]

Values  
\[ v ::= k \mid x. \; e \mid \langle v, v \rangle \mid v \langle I \rangle \mid a \]

Casted Values  
\[ cv ::= v \mid (cv, cv) \]

Heap  
\[ \mu ::= \emptyset \mid \mu(a \mapsto v : T) \]

Evolving Heap  
\[ \nu ::= \emptyset \mid \nu(a \mapsto cv : T) \]

Frames  
\[ F ::= \ldots \]

Expression typing  
\[ \Gamma; \Sigma \vdash e : T \]

State reduction rules

For

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>Error</td>
</tr>
</tbody>
</table>

Monotonic references without blame

Cast reduction rules

Program reduction rules

For \( X \in \{ cr, e \} \):

State reduction rules

\[ \vdash e : T \]

\[ T \cap T = T \]

\[ T \cap \ast = T \]

\[ B \cap B = B \]

\[ (T_1 \times T_2) \cap (T_1 \times T_3) = (T_1 \cap T_3) \times (T_2 \cap T_4) \]

\[ (T_1 \times T_2) \cap (T_3 \times T_4) = (T_1 \times T_3) \times (T_2 \times T_4) \]

Figure 7. The meet function (greatest lower bound)

source type of the cast don’t match! In fact, in this example the result would be incorrect: we would get 42(Int!) instead of 42.

There are several solutions to this problem, and they all require storing more information on the heap or as a separate map. Here we take the most straightforward approach of immediately updating the heap with casted values, that is, with values that are in the process of being cast.

We walk through the execution of the above example, explaining our rules for reducing casted values in the heap and showing snapshots of the heap. We use the following abbreviations.

\[ a_0 \Rightarrow (42\langle Int! \rangle, 7\langle Int! \rangle, 0\langle Int! \rangle) : T_0 \]

The second line sets the third element to be a reference to itself.

\[ a_0 \Rightarrow (42\langle Int! \rangle, 7\langle Int! \rangle, a_0\langle \text{Ref} T_0! \rangle) : T_0 \]

The third line casts the reference to \( T_1 \) via (CASTREF1).

\[ a_0 \Rightarrow (42\langle Int! \rangle, 7\langle Int! \rangle, a_0\langle \text{Ref} T_0! \rangle)\langle c \rangle : T_1 \]

We have a casted value in the heap that needs to be reduced. We apply (HCast) and (PURECAST) to get

\[ a_0 \Rightarrow (42, 7\langle Int! \rangle, a_0\langle \text{Ref} T_2 \rangle) : T_1 \]

We cast address \( a_0 \) again, this time to \( T_1 \times T_2 \), via rule (HDROP) and (CASTREF1).

\[ a_0 \Rightarrow (42, 7\langle Int! \rangle, a_0\langle \text{Ref} T_2 \rangle \langle c \times \text{Ref} T_2 \rangle : T_1 \times T_2 \times \text{Ref} T_2 \]

A few reductions via (HCast) and (PURECAST) give us

\[ a_0 \Rightarrow (42, 7, a_0\langle \text{Ref} T_2 \rangle) : \text{Int} \times \text{Int} \times \text{Ref} T_2 \]

The final cast applied to \( a_0 \) is a no-op because the run-time type is already less dynamic than \( T_2 \). So we reduce via (HCast) and (CASTREF2) to:

\[ a_0 \Rightarrow (42, 7, a_0\langle \text{Ref} T_2 \rangle) : \text{Int} \times \text{Int} \times \text{Ref} T_2 \]

Even though we allow casted values on the heap, we require the normalization of all such casts before returning to the execution of the program. We distinguish between normal heaps of values, \( \mu \), and evolving heaps, \( \nu \), that may contain both values and casted values. Normal heaps are a subset of the evolving heaps.

4. Type Safety for Monotonic References

We present the high-points of the type safety proof here. The full 26-page formal development and proof is mechanized in Isabelle 2013 and can be found in the supplementary material. The semantics in the mechanized version differs from the semantics presented.
Proof sketch. Let $\Sigma$ be a well-typed heap. The most interesting proofs are for the reduction relations. The most interesting proofs are for the reduction relations. The most interesting proofs are for the reduction relations. The most interesting proofs are for the reduction relations. The most interesting proofs are for the reduction relations. The most interesting proofs are for the reduction relations. The most interesting proofs are for the reduction relations.

Figure 8. Compile casts to monotonic coercions (without blame)

here in that it uses an abstract machine instead of a reduction semantics, as we found the mechanized proof easier to carry out on an abstract machine. The differences between a reduction semantics and an abstract machine are not important, as one can be derived from the other (Biermann and Danvy 2009).

We begin by lifting the less-dynamic relation to heap typings.

**Definition 4** (Less-dynamic relation on heap typings). $\Sigma' \subseteq \Sigma$ iff $dom(\Sigma') = dom(\Sigma)$ and $\Sigma(a) = T$ implies $\Sigma'(a) = T'$ where $T' \subseteq T$.

Our first lemma below is important: expression typing is preserved when moving to a less-dynamic heap typing. This allows us to make monotonically-decreasing updates to the heap.

**Lemma 5** (Strengthening w.r.t. the heap typing). If $\Gamma; \Sigma \vdash e : T$ and $\Sigma' \subseteq \Sigma$, then $\Gamma; \Sigma' \vdash e : T$.

**Proof sketch.** The interesting case is for addresses. We have

$$\Sigma(a) \subseteq T ; \Sigma \vdash a : T$$

From $\Sigma' \subseteq \Sigma$ and transitivity of $\subseteq$ (Proposition 1), we have $\Sigma'(a) \subseteq T$. Therefore $\Gamma; \Sigma' \vdash a : T$.

The definition of well-typed heaps is standard.

**Definition 6** (Well-typed heaps). A heap $\nu$ is well-typed with respect to heap typing $\Sigma$, written $\Sigma \vdash \nu$, iff $\forall a. \Sigma(a) = T$ implies $\nu(a) = cv : T$ and $\nu(a) = \nu$.

From the strengthening lemma, we have the following corollary.

**Corollary 7** (Monotonic heap update). If $\Sigma \vdash \nu$ and $\Sigma(a) = T$ and $T' \subseteq T$ and $\nu(a) = cv : T$ for some $cv$.

**Proof sketch.** Let $\Sigma' = \Sigma(a \mapsto T')$. From $T' \subseteq T$ we have $\Sigma' \subseteq \Sigma$, so by Lemma 5 we have $\nu(a) = cv : T'$ and $\nu(a) = \nu$. Thus, $\Sigma(a \mapsto T') \vdash \nu(a) = cv : T'$.

**Lemma 8** (Progress and Preservation). Suppose $\emptyset; \Sigma \vdash e : T$ and $\Sigma \vdash \nu$. Exactly one of the following holds:

1. $e$ is a value, or
2. $e = \text{error}$, or
3. $e, \nu \rightarrow e', \nu'$ for some $e'$ and $\nu'$.

Also, for any $e', \nu'$, if $e, \nu \rightarrow e', \nu'$ then $\emptyset; \Sigma' \vdash e' : T$ and $\Sigma' \vdash \nu'$ and $\Sigma' \subseteq \Sigma$ for some $\Sigma'$.

**Proof sketch.** We prove progress and preservation for each of the reduction relations. The most interesting proofs are for the reduction rules that concern casting references. We give the proofs for those cases here.

Case (CastRef1):

$$\nu(a) = cv : T_1 ; T_3 = T_3 \cap T ; T_3 \neq T_1 ; cv' = cv(T_1 \Rightarrow T_3)$$

$$\alpha(Ref\mathcal{T}), \nu \rightarrow_{cv} \alpha(Ref\mathcal{T})$$

Take $e' = a, \nu' = \nu(a \Rightarrow cv' : T_3)$, and $\Sigma' = \Sigma(a \Rightarrow T_3)$. We have $\Sigma'(a) = T_3$ and $T_3 \subseteq T$ (by Proposition 3), so $\emptyset; \Sigma' \vdash a : T$. Also, from $T_3 \subseteq T$ we have $\Sigma' \subseteq \Sigma$. With $T_3 \subseteq T_1$ (by Proposition 3) we conclude $\Sigma' \vdash \nu'$ by Corollary 7.

Case (CastRef2):

$$\nu(a) = cv : T_1 ; T_1 = T_3 \cap T$$

$$\alpha(Ref\mathcal{T}), \nu \rightarrow_{cv} a, \nu$$

Take $e' = a, \nu' = \nu$, and $\Sigma' = \Sigma$. We trivially have $\Sigma' \vdash \nu'$, so we just need to show that $\Sigma' \vdash a : T$. From $\Sigma' \vdash \nu'$ and $\nu'(a) = cv : T_1$ we have $\Sigma'(a) = T_1$. From $T_1 = T_1 \cap T$ we have $T_1 \subseteq T$ (by Proposition 3). Thus, we conclude that $\Sigma' \vdash a : T$.

**Theorem 9** (Type Safety). Suppose $\emptyset; \Sigma \vdash e : T$ and $\Sigma \vdash \nu$.

Exactly one of the following holds:

1. $e, \nu \rightarrow^* \text{error}, \nu'$, or $e, \nu \rightarrow^* e', \nu'$.
2. $e, \nu \rightarrow^* \text{error}, \nu'$, or $e, \nu \rightarrow^* e', \nu'$.
3. $e$ diverges.

**Proof.** If $e$ diverges we immediately conclude the proof. Otherwise, suppose $e$ does not diverge. Then $e, \nu \rightarrow^* e', \nu'$ and $e'$ cannot reduce. We proceed by induction on the length $e, \nu \rightarrow^* e', \nu'$, and use Lemma 8 to conclude.

5. **Monotonic References with Blame**

We turn to the challenge of designing blame tracking for monotonic references, presenting several examples that motivate and provide intuitions for the design. The later part of this section presents the dynamic semantics of monotonic references with blame tracking.

Consider the following example in which we allocate a reference of dynamic type and then, separately, cast from $\textbf{Ref } \ast$ to $\textbf{Ref Int}$ and to $\textbf{Ref Bool}$.

```plaintext
let r0 = ref (42 as int*) in
let r1 = r0 as int Ref Int in
let r2 = r0 as int Ref Bool in

!r2
```

With monotonic references, the cast at $\ell_3$ triggers an error, because $\textbf{Int}$ and $\textbf{Bool}$ are inconsistent. But what blame labels should the error message include? Is it only the fault of $\ell_3$? Not really; because $\ell_3$ would not cause an error if it were not for the cast at $\ell_2$.

The casts at $\ell_2$ and $\ell_3$ disagree with each other regarding the type of the heap cell, so we blame both. The result of this program is blame $\{\ell_2, \ell_3\}$.

Next consider an example in which we allocate a reference at type $\textbf{Ref Int}$, cast it to $\textbf{Ref } \ast$, and then attempt to write a Boolean.

```plaintext
let r0 = ref 42 in
let r1 = r0 as int Ref * in
r1 := e3 (true as int *)
```

The update on the third line triggers an error, and we have three possible locations to blame: $\ell_3$, $\ell_2$, and $\ell_3$. The cast at $\ell_2$ is from $\textbf{Bool}$ to $\ast$, which is harmless. There is no cast at $\ell_3$, we are just writing a value of type $\ast$ to a reference of type $\textbf{Ref } \ast$. The real culprit here is $\ell_3$, which casts from $\textbf{Ref Int}$ to $\textbf{Ref } \ast$, thereby opening up the potential for the later cast error. Naively, this looks like an upcast, but a proper treatment of subtyping for references makes references invariant. So we have $\textbf{Ref Int} \not\sqsubset \textbf{Ref } \ast$ and
This subtyping relation is for the D variant of blame tracking, and not the fourth line. We allocate a reference to a pair at type integer, whereas in the second example we write an integer and a we update through the original reference, writing a Boolean and and here is the second example, just showing the fourth line: blame
which we shall explain later in this section. In the above examples, Figure 10 gives the syntax of labeled types and operations on them, each type constructor within the type can be labeled with a type.

\[
\begin{array}{ccc}
B <: B & T <: \star & \text{Ref } T <: \text{Ref } T \\
T_1' <: T_1 & T_2 <: T_2' & T_1' \to T_2' <: T_1' \times T_2'
\end{array}
\]

Figure 9. Subtyping relation

the result of this program is blame \{\ell_1\}. Figure 9 presents the subtyping relation\(^1\).

We consider a pair of examples below that differ only on the fourth line. We allocate a reference to a pair at type Ref (* \star *) then cast it to Ref (Int \times \star) and to Ref (* \times Int). In the first example, we update through the original reference, writing a Boolean and integer, whereas in the second example we write an integer and a Boolean. Here is the first example:

\[
\begin{align*}
\text{let } r_0 &= \text{ref}(1 \text{ as } \ell_1', 2 \text{ as } \ell_2') \text{ in} \\
\text{let } r_1 &= r_0 \text{ as } \ell_3 \text{ Ref (Int } \times \star) \text{ in} \\
\text{let } r_2 &= r_0 \text{ as } \ell_4 \text{ Ref (* } \times \text{ Int) in} \\
\text{let } r_5 &= (\text{true as } \ell_5', 2 \text{ as } \ell_6') \\
\text{fst } r_0
\end{align*}
\]

and here is the second example, just showing the fourth line:

\[
\begin{align*}
\text{...} \\
r_0' &= (1 \text{ as } \ell_1', \text{true as } \ell_2') \\
\text{...}
\end{align*}
\]

The first example should produce blame \{\ell_3\} while the second example should produce blame \{\ell_2\}, but the challenge is how can we associate multiple blame labels with the same heap cell?

We take inspiration from Siek and Walder (2010) and use labeled types for our run-time type information. With a labeled type, each type constructor within the type can be labeled with a type. Figure 10 gives the syntax of labeled types and operations on them, which we shall explain later in this section. In the above examples, the run-time type information for the heap cell evolves in the following way:

\[
(*) \Rightarrow (\text{Int}^{\ell_1} \times \beta) \Rightarrow (\text{Int}^{\ell_1} \times \beta \text{ Int}^{\ell_2})
\]

In the first example, when we write true into the first element of the pair, the cast to Int fails and blames \ell_3, as desired. In the second example, when we write true into the second element of the pair, the cast to Int fails and blames \ell_4, as desired.

Our next example brings up a somewhat ambiguous situation. We allocate a reference at type Ref \star, cast it to Ref Int twice, then write a Boolean.

\[
\begin{align*}
\text{let } r_0 &= \text{ref}(42 \text{ as } \ell_1') \text{ in} \\
\text{let } r_1 &= r_0 \text{ as } \ell_2 \text{ Ref Int in} \\
\text{let } r_2 &= r_0 \text{ as } \ell_3 \text{ Ref Int in} \\
\text{let } r_0' &= (\text{true as } \ell_4')
\end{align*}
\]

Should we blame \ell_2 or \ell_3? In some sense, they are both just as guilty and the ideal would be to blame them both. On the other hand, maintaining potentially large sets of blame labels would induce some space overhead. Our design instead blames the first cast with respect to execution order, in this case \ell_2.

For our final example, we adapt the above example to have a function in the heap cell so that we can consider the behavior to the left of the arrow.

\[
\begin{align*}
\text{let } r_0 &= \text{ref}(\lambda x: \star . \text{true}) \text{ in} \\
\text{let } r_1 &= r_0 \text{ as } \ell_1 \text{ Ref (Int } \to \text{ Bool) in} \\
\text{let } r_2 &= r_0 \text{ as } \ell_2 \text{ Ref (Int } \to \text{ Bool) in} \\
r_0' &= \text{Ref (true as } \ell_3') \\
\text{let } r_0' \text{ as } \ell_0 \text{ Ref (true as } \ell_3')
\end{align*}
\]

The run-time type information for the heap cell evolves in the following way:

\[
(*) \Rightarrow (\text{Int}^{\ell_1} \to \beta \text{ Bool}) \Rightarrow (\text{Int}^{\ell_1} \to \beta \text{ Bool})
\]

The function application on the last line of the example triggers a cast error, with the blame going to \ell_1, again because we wish to blame the first cast with respect to execution order. However, to obtain this semantics some care must be taken. On the second cast, we merge the labeled type for the second cast with the current run-time type information:

\[
(\text{Int}^{\ell_1} \to \beta \text{ Bool}) \bowtie (\text{Int}^{\ell_2} \to \beta \text{ Bool})
\]

If we were to use the composition function from Siek and Walder (2010), the result would be Int^{\ell_2} \to \beta \text{ Bool} because that composition function is contravariant for function parameters. Here we instead want to be covariant on function parameters, so the result is Int^{\ell_1} \to \beta \text{ Bool}. We define a new function for merging labeled types, \bowtie, in Figure 10.

Semantics of monotonic references with blame

Armed with the intuitions from the above examples, we discuss the semantics of monotonic references with blame, defined in Figure 12. The semantics is largely similar to the semantics without blame except that the run-time type information is represented as labeled types and we replace the functions, such as meet (\cap) that operate on types, with functions such as merge (\bowtie) that operate on labeled types.

**Proposition 10** (Meet is the erasure of merge).

If \(|P_1| \sim |P_2|, \text{ then } (P_1 \bowtie P_2) = |P_1| \cap |P_2|.

If \(|P_1| \not\sim |P_2|, \text{ then } P_1 \bowtie P_2 = L^{-}\text{ for some } L.

As discussed with the example above, the definition of \(P_1 \bowtie P_2\) takes into account that \(P_1\) is temporally prior to \(P_2\) and should therefore take precedence with respect to blame responsibility. We use the auxiliary function \(p \bowtie q\) to choose between two optional labels, returning the first if it is present and the second otherwise.

When we cast a reference via rule (6), we need to update the heap cell from labeled type \(P_1\) to \(P_3\). We accomplish this with a new operator \(P_1 \Rightarrow P_3\) that produces a coercion. The most interesting line of its definition is for reference types. There we use a different operator, \(P \bowtie Q\), that produces a labeled type and captures the bidirectional read/write nature of mutable references.

The definitions of \(\bowtie\), \(\Rightarrow\), and \(\bowtie\) need to percolate errors, which we write as \(L^{-}\) where \(L\) is a set of blame labels. We use “smart” constructors \(\Rightarrow\), \(\bowtie\), and \(\bowtie\) that return \(L^{-}\) if either argument is \(L^{-}\) (with precedent to the left if both arguments are errors), but otherwise act like the underlying constructor.

In the rule for allocation, we initialize the RTTI to \(T^0\). (Figure 11 defines converting a type to a labeled type.) In the rule for a dynamic dereference, (DYNDRefMB), we cast from the reference’s run-time labeled type to \(T\) by promoting \(T\) to the labeled type \(T^0\) and then applying the \(\Rightarrow\) function to cast between labeled types, so we have \(u(a)\text{mt} \Rightarrow T^0\). Suppose that \(u(a)\text{mt} = \text{Ref Int}^1\) and \(T = \text{Ref } x\). Then the coercion we apply during the dereference is \(\text{Int}^1\); so our injection coercions contain labeled types. The rule for dynamic update, (DYNUpdMB), is dual: we perform the cast \(T^0 \Rightarrow u(a)\text{mt}\).

---

\(^1\) This subtyping relation is for the D variant of blame tracking, and not the more common UD (Siek et al. 2009).
Optional labels \( p, q \) ::= \( \emptyset \mid \{ \ell \} \)

Label sets \( L \) ::= \( \emptyset \mid \ell \mid \{ \ell_1, \ell_2 \} \)

Labeled types \( P, Q \)::= \( B^p \mid P \rightarrow^p P \mid P \times^p P \mid \text{Ref}^p P \mid * \)

Erase labels \( |P| = T \)

\[ |B^p| = B \quad |P \rightarrow^p Q| = |P| \rightarrow |Q| \quad |P \times^p Q| = |P| \times |Q| \]

\[ |\text{Ref}^p P| = \text{Ref} |P| \quad |*| = * \]

Top label \( \text{lab}(B^p) = p \quad \text{lab}(P \rightarrow^p Q) = p \quad \text{lab}(P \times^p Q) = p \)

\[ \text{lab}(\text{Ref}^p P) = p \quad \text{lab}(*|) = \emptyset \]

Merge optional labels \( \{ \ell \} \triangle q = \{ \ell \} \quad \emptyset \triangle q = q \)

Merge labeled types \( P \triangle P = P \) or \( \perp^L \)

\[ B^p \triangle B^q = B^{p \oplus q} \]

\[ P \triangle * = P \]

\[ * \triangle Q = Q \]

\[ (P \rightarrow^p P') \triangle (Q \rightarrow^q Q') = (P \triangle Q) \rightarrow^{p \oplus q}(P' \triangle Q') \]

\[ (P \times^p P') \triangle (Q \times^q Q') = (P \triangle Q) \times^{p \oplus q}(P' \triangle Q') \]

\[ \text{Ref}^p P \triangle \text{Ref}^q Q = \text{Ref}^{p \oplus q} (P \triangle Q) \quad \text{otherwise} \]

Bidirectional cast between labeled types \( P \Leftrightarrow P = P \) or \( \perp^L \)

\[ B^p \leftrightarrow B^q = B^\delta \]

\[ P \leftrightarrow * = P \]

\[ * \leftrightarrow Q = Q \]

\[ (P \rightarrow^p P') \leftrightarrow (Q \rightarrow^q Q') = (P \leftrightarrow Q) \rightarrow^{p \leftrightarrow q} (P' \leftrightarrow Q') \]

\[ (P \times^p P') \leftrightarrow (Q \times^q Q') = (P \leftrightarrow Q) \times^{p \leftrightarrow q} (P' \leftrightarrow Q') \]

\[ \text{Ref}^p P \leftrightarrow \text{Ref}^q Q = \text{Ref}^{p \leftrightarrow q} (P \leftrightarrow Q) \quad \text{otherwise} \]

Cast between labeled types \( P \Rightarrow P = \epsilon \) or \( \perp^L \)

\[ B^p \Rightarrow B^q = \perp \]

\[ * \Rightarrow * = \perp \]

\[ P \Rightarrow * = P! \]

\[ * \Rightarrow Q = Q? \]

\[ (P \rightarrow^p P') \Rightarrow (Q \rightarrow^q Q') = (Q \Rightarrow P) \rightarrow (P' \Rightarrow Q') \]

\[ (P \times^p P') \Rightarrow (Q \times^q Q') = (P \Rightarrow Q) \times (P' \Rightarrow Q') \]

\[ \text{Ref}^p P \Rightarrow \text{Ref}^q Q = \text{Ref} (P \Rightarrow Q) \quad \text{otherwise} \]

\[ P \Rightarrow Q = \perp^{\text{lab}(P), \text{lab}(Q)} \]

\[ (T \Rightarrow^\ell T) = \epsilon \]

\[ (B \Rightarrow^\ell B) = \ell \]

\[ (* \Rightarrow^\ell *) = \ell \]

\[ (T \Rightarrow^\ell *) = T^\delta! \]

\[ (* \Rightarrow^\ell T) = T^\delta? \]

\[ (T_1 \Rightarrow T_2) \Rightarrow (T'_1 \Rightarrow T'_2) = (T'_1 \Rightarrow T_1) \Rightarrow (T_2 \Rightarrow T'_2) \]

\[ (T_1 \times T_2) \Rightarrow (T'_1 \times T'_2) = (T'_1 \Rightarrow T'_1) \times (T_2 \Rightarrow T'_2) \]

\[ \text{Ref} T_1 \Rightarrow^\ell \text{Ref} T_2 = \text{Ref} (T'_1 \Leftrightarrow T'_2) \]

Add labels to a type \( B^\ell = B^\delta \quad (T_1 \Rightarrow T_2) = T'_1 \Rightarrow T'_2 \quad (T_1 \times T_2) = T'_1 \times T'_2 \)

\[ \text{Ref} T^\ell = \text{Ref}^\ell \text{Ref}^\delta \]

\[ *^\ell = * \]

Figure 11. Compile casts to monotonic coercions (with blame)

Because our injection and projection coercions contain labeled types, the \textsc{(Collapse)} rule becomes

\[ v(P_1 \mid P_2 \mid \ldots) \rightarrow_c v(P_1 \Rightarrow P_2) \quad \text{if } |P_1| \sim |P_2| \]

We make similar changes to the \textsc{(Conflict)} rule.

Figure 11 defines the compilation of casts to monotonic coercions. Compared to the compilation without blame (Figure 8), there are three differences. The first two concern injection and projection coercions: instead of only having a blame label on projections we have labeled types inside both injections and projections, as noted above. In the compilation of a cast labeled \( \ell \), we generate a labeled type for the injection from \( T \) by adding the empty label to \( T \); and for the projection to \( T \) by adding \( \ell \) to \( T \). The third difference is in the formation of the reference coercion. Instead of simply taking the target type, we use the bidirectional operator \( \Leftrightarrow \). Recall the second example of this section in which we blamed the cast from \( \text{Ref} \text{Int} \leftrightarrow \text{Ref} \). By using \( \Leftrightarrow \), the resulting coercion is \( \text{Ref} \text{Int}^\ell \) instead of \( \text{Ref} \).

6. The Blame-Subtyping Theorem

The blame-subtyping theorem pin-points the source of cast errors in gradually-typed programs. The blame-subtyping theorem states that if a program results in a cast error, blame \( L \), then the blame labels in \( L \) identify the location of implicit casts that did not respect subtyping. Or put positively, the blame labels that occur in safe implicit casts, that is, casts \( T_1 \Rightarrow T_2 \) where \( T_1 <_c T_2 \), can never be blamed.

We prove the blame-subtyping theorem via a preservation-style proof (Wadler and Findler 2007, 2009) in which we preserve the \( \epsilon \) safe \( \ell \) predicate, a technique due to Siek (2008). This proof will be conducted on the coercion calculus, so to relate the result back to the gradually-typed \( \lambda \) calculus, we need a theorem concerning the relationship between subtyping and coercion blame safety, Theorem 12. Recall that subtyping is defined in Figure 9 and the compilation to coercions is defined in Figure 11. The safe predicate is defined for labeled type, coercions, expressions, and states in Figure 13.

The compilation to coercions relies on the auxiliary function \( \Leftrightarrow \) in the case for reference types, so to prove the subtyping and coercion safety theorem, we need the following lemma.

**Lemma 11** (Reflexivity of \( \Leftrightarrow \) and blame).

For all \( P \) and \( \ell \), \( (P \Rightarrow P) \) safe \( \ell \).
Syntax

Expressions $e ::= \cdots \mid \text{blame } L$

Coercions $e ::= t \mid P ? \mid P ! \mid \text{c} \in e \mid c \times e \mid e : e \mid \text{Ref } P$

Values $v ::= k \mid \lambda x.e \mid (v,v) \mid v(P) \mid a$

Heap $\mu ::= \emptyset \mid \mu(a \mapsto v : P)$

Evolving Heap $\nu ::= \emptyset \mid \nu(v(a \mapsto cv : P))$

Coercion typing $\text{c} : T \Rightarrow T$

Pure cast reduction rules $e \rightarrow_{c} e'$

Cast reduction rules $e \rightarrow_{c,r} \nu$

Program reduction rules $e, \nu \rightarrow_{r} e, \nu$

For $X \in \{c,r,e\}$, $F[e], \nu \rightarrow_{X} F[e'], \nu'$

State reduction rules $e, \mu \rightarrow_{s} e', \nu$

Figures 12 and 13. Definition of the safety predicate

Proof. Straightforward by inspection on the definition of $\leftrightarrow$. 

Theorem 12 (Subtyping and blame safety). For all $T_1$, $T_2$, and $\ell$, it holds that $T_1 \bowtie T_2$ iff $(T_1 \Rightarrow^\ell T_2)$ safe $\ell$.

Proof sketch. We prove the forward direction of the implication by induction on the compilation $(T_1 \Rightarrow^\ell T_2)$. We show only the case for the type Ref, as it relies on the operator $\leftrightarrow$.

Case Ref $T_1 \Rightarrow^\ell$ Ref $T_2$. By definition of $\bowtie$, we have Ref $T_1 \bowtie$ Ref $T_2$ only when $T_1 = T_2$. By Lemma 11 we have that $(T_1 \Rightarrow^\ell T_2)$ safe $\ell$, and thus (Ref $T_1 \Rightarrow^\ell$ Ref $T_2$) safe $\ell$.

We prove the backward direction of the implication by induction on $(T_1 \Rightarrow^\ell T_2)$ safe $\ell$. We show only the case for the type $\rightarrow$ for it is contravariant.

Case $T_1 \rightarrow T_2$ is straightforward. To prove this, we need to derive $(T_3 \Leftrightarrow T_1)$ and $(T_3 \Leftrightarrow T_2)$. By the induction hypothesis we know that $(T_1 \Rightarrow^\ell T_2)$ safe $\ell$. By definition, this means that $(T_1 \Rightarrow^\ell T_1) \Rightarrow (T_2 \Rightarrow^\ell T_2)$ safe $\ell$. And therefore $(T_3 \Rightarrow^\ell T_1)$ safe $\ell$ and $(T_2 \Rightarrow^\ell T_2)$ safe $\ell$. By induction we thus have $(T_3 \Leftrightarrow T_1)$ and $(T_2 \Leftrightarrow T_2)$. 

The key to proving the preservation of blame safety for the coercion calculus is showing that our operators on labeled types preserve blame.

Lemma 13 (Blame safety for $\bowtie$, $\Rightarrow$ and $\leftrightarrow$). For all $P$ and $Q$, if $P$ safe $\ell$ and $Q$ safe $\ell$ then $P \leftrightarrow Q$ safe $\ell$ for $\leftrightarrow \in \{\bowtie, \Rightarrow, \leftrightarrow\}$.

Proof. For each operator, we prove blame safety by a straightforward induction. The only non-trivial case is the Ref type for $\Rightarrow$, i.e. Ref $P \Rightarrow$ Ref $Q$ is Ref $P \leftrightarrow Q$, as it relies on the operator $\leftrightarrow$. In this case we do not appeal to induction but to the blame safety for $\leftrightarrow$, which can be proved easily as $\leftrightarrow$ does not rely on other operators.
Lemma 14 (Preservation of blame safety). For all e, e', ν, ν', and ℓ, it holds that if e, ν safe ℓ and e, ν → ℓ e', ν' then e', ν' safe ℓ.

Proof. We prove blame safety for each of the reduction relations by induction on their derivation. We here show only the most involved cases. 
Case (PCAST):
\[
\nu(a) = cv : P_1 \quad P_3 = P_1 \triangleq P_2 \\
|P_3| ≠ |P_1| \\
cv' = cv(P_1 \Rightarrow P_3)
\]
By assumption we have ν safe ℓ. Thus, we can infer cv safe ℓ and P₁ safe ℓ. By assumption we also have (ref P₂) safe ℓ, and therefore P₂ safe ℓ. Because P₁ = P₁ ∆ P₂, by Lemma 13 (Blame Safety for ∆) we infer P₁ safe ℓ. Now, by Lemma 13 (Blame Safety for ⇒), we have P₁ ⇒ Pᵢ safe ℓ. Therefore cv' = cv(P₁ ⇒ Pᵢ) safe ℓ. Now, it is easy to see that a, ν(a ⇒ cv' : P₃) safe ℓ, as ν safe ℓ by assumption and both cv' safe ℓ and P₃ safe ℓ as inferred above.

(DYNUPDMB):
\[
a := v[0 : T] ; \mu \rightarrow e a, \mu(a ⇒ cv : μ(a)_{mi})
\]
where cv = v(T⁰ ⇒ μ(a)_{mi}). By assumption we have μ, v, and T safe for ℓ. We therefore can infer μ(a)_{mi} safe ℓ. Also, we can apply Lemma 13 (Blame Safety for ⇒) to get T⁰ ⇒ μ(a)_{mi} safe ℓ. Therefore cv = v(T⁰ ⇒ μ(a)_{mi}) safe ℓ. Finally, we conclude that a, μ(a ⇒ cv : μ(a)_{mi}) safe ℓ.

Proof. From the assumptions we have e safe ℓ by Lemma 18. Then we conclude by applying the Blame-Subtyping Theorem for the coercion calculus.

7. Implementation concerns wrt. strong updates
The monotonic semantics for references performs in-place updates to the heap with values of different type. In languages where values have uniform type, like many functional and object-oriented languages, this does not pose a problem. However, for languages where values may have different sizes, in-place updates do pose a problem. We recently discovered a solution inspired by garbage collection techniques. When the semantics says to do an in-place update with a larger value, what the implementation can do is allocate a new piece of memory and place a forwarding pointer in the old location. When reading and writing through dynamic references, the implementation would need to check for and follow the forwarding pointers. However, when reading and writing through fully-static references, the implementation would not need to worry about forwarding pointers because a fully-static heap cell is never moved. Also, during a garbage collection the implementation could collapse sequences of forwarding pointers to reduce the overhead of them in the subsequent execution.

8. Related Work
Interest in integrating static and dynamic typing within the same language has existed for some time, and early approaches included the addition of a dynamic type to a static type system (Abadi et al. 1989) as well as the quasi-static typing of Thatte (1990).

Siek and Taha (2006) introduced the term “gradual typing” to describe such systems, and were the first to study the interaction between gradual typing and mutable references, but used an inflexible consistency relation that did not allow implicit casts between references of different type. Herman et al. (2007, 2010) relaxed the consistency rule for references and introduced the standard semantics, in which casting a reference creates a proxied reference that performs casts on every read and write.

Henglein (1994) developed the coercion calculus to aid in understanding the compilation of dynamically-typed languages to statically typed ones. Herman et al. (2007, 2010) used it to design a space-efficient approach to casts in gradually-typed languages. Siek et al. (2009) introduced several approaches to integrating blame tracking into the coercion calculus, and Siek and Wadler (2010) introduced threesomes, which similarly can represent sequences of casts in a space-efficient manner with blame tracking.

The casts and coercions studied in this paper bear many similarities with contracts (Findler and Felleisen 2002). Racket (Flatt and PLT 2014) provides contracts for mutable values in the form of impersonators (Strickland et al. 2012), which, for our purposes, can be viewed as implementing the standard semantics of Herman et al. (2007), as we saw in Section 2.

Fähndrich and Leino (2003) introduce a technique similar to monotonic references with their monotonic typestate. In this design, objects may flow from less restrictive to more restrictive type states, but not vice versa. Unlike monotonic references, which require runtime checks due to the existence of dynamically-typed regions of code, in their system monotonicity is enforced statically.

Swamy et al. (2014) design a gradually-typed variant of JavaScript named TS', that is type safe despite interacting with untrusted JavaScript contexts that can walk the stack, use eval, and perform prototype poisoning. They use an RTTI-based approach to cast objects, similar to the way we associate RTTI with references. Swamy et al. (2014) allow their heap to evolve monotonically, but with respect to subtyping instead of the less-dynamic relation as we do. TS' compiles to JavaScript and therefore inherits all of the
overheads of dynamic typing, even in statically-typed regions of code. Finally, TS does not perform blame tracking whereas we have showed how to perform blame tracking for monotonic references and proved the blame-subtyping theorem.

Gradual typing was added to C with the addition of the dynamic type (Hejlsberg 2010). Bierman et al. (2010) define a formal model of C, named FC, and present an operational semantics. The semantics is similar to that of Swamy et al. (2014) in that they use an RTTI-based approach and subtype checks to implement casts.

Many gradually-typed systems sidestep this issue entirely by employing a type-erasure semantics, that is, they implement a gradual type checker but do not insert run-time casts (Hejlsberg 2012). The advantage of the type-erasure semantics is its ease of implementation and lack of run-time overhead (beyond the normal amount for a dynamically-typed language), but the disadvantage is that one gives up a static notion of type soundness and there remains run-time overhead in fully-static code.

9. Conclusion
We have presented a new design for gradually-typed mutable references, called monotonic references; the first to incur zero-overhead for reference accesses in statically typed code while maintaining the full expressiveness of a gradual type system. Further, the design does not use reference proxies, so it does not disrupt object identity. We defined a dynamic semantics for monotonic references and presented a mechanized proof of type safety. Further, we defined blame tracking based on using labeled types in the run-time type information and proved the blame-subtyping theorem.

References


