Gradual Typing for Mutable Objects

Jeremy G. Siek¹, Michael M. Vitousek², and Shashank Bharadwaj¹

¹ Department of Electrical, Computer, and Energy Engineering
² Department of Computer Science
University of Colorado Boulder
Boulder, CO 80309, USA
{jeremy.siek,michael.vitousek,shashank.bharadwaj}@colorado.edu

Abstract. Gradual typing enables a mixture of static and dynamic typing within the same program. There are four properties that are desirable in a gradually-typed language: 1) the type system allows implicit conversions to and from the dynamic type so that values can easily pass between statically and dynamically-typed regions of code, 2) the overhead associated with implicit conversions is low, 3) if one of these conversions fails, the guilty source location is blamed, and 4) statically-typed regions of code execute just as efficiently as code written in a statically-typed language. This paper presents the first design, monotonic objects, that has all four properties in the presence of mutable state. On the way to this design we develop guarded objects, a natural extension of earlier work that imposes some overhead on statically-typed regions of code.

1 Introduction

Despite the polarizing affect that static and dynamic typing has on programmers, the last decade has seen a renewed interest by researchers to integrate the two [Anderson and Drossopoulou, 2003, Flanagan et al., 2006, Tobin-Hochstadt and Felleisen, 2006, Wadler and Findler, 2009, Bierman et al., 2010, Wrigstad et al., 2010, Bayne et al., 2011]. This paper concerns the gradual typing approach to this integration [Siek and Taha, 2006, Herman et al., 2007, Ina and Igarashi, 2011, Wolff et al., 2011, Takikawa et al., 2012, Rastogi et al., 2012]. Attesting to the practical utility of gradual typing, three of Microsoft’s languages, Visual Basic, C#, and TypeScript, provide gradual typing to some degree.

The goal of gradual typing is to let programmers enjoy the benefits of either typing discipline within different regions of a program. The statically typed regions should benefit from efficient execution and from the early detection of type-related bugs. The dynamically typed regions should benefit from increased flexibility and reflection. But there is a tension between these design goals, particularly in languages with mutable state. In this paper we explore two new points in the design space for mutable objects, including the first design that enables the seamless integration of statically and dynamically-typed regions of code while preserving the efficient execution of statically-typed regions.
At the heart of gradual typing is a *consistency* relation on types, written $T_1 \sim T_2$, that allows implicit conversions to and from the dynamic type, written $\star$, while disallowing conversions between inconsistent types such as int and string [Siek and Taha, 2006]. The consistency relation is orthogonal to subtyping, and to support both subtyping and consistency one can compose the two relations [Siek and Taha, 2007]. The dynamic semantics of gradual typing is defined by a translation to an intermediate language with explicit casts.

The original treatment of mutable state by Siek and Taha [2006] leaves something to be desired because it did not allow for the passing of ML-style references between static and dynamic code. The consistency rule, shown to the right, required the underlying type $T$ to be invariant. Programs could not pass a reference of type $\text{ref int}$ to a function expecting $\text{ref } \star$. On the positive side, the semantics of Siek and Taha [2006] does enable the fast execution of statically-typed code. The canonical forms lemma only admits one kind of value per type, and correspondingly, there is only one reduction rule for each elimination form. Thus, there is no need to dispatch on the kind of value. However, there is another efficiency concern: the cost of passing values between static and dynamic regions. Every application of a cast to a function creates a wrapper, and a function may be cast many times using unbounded space.

Herman et al. [2007] solve both the space efficiency issue and the problem with casting references. They represent casts using the Coercion Calculus of Henglein [1994] in which sequences of coercions normalize to coercions of at most length 3. Herman et al. [2007] enable the casting of references by using the more permissive consistency rule shown on the right and by creating a new form of coercion, $\text{ref } c_1 c_2$, to represent casts between reference types. The coercion $c_1$ is used when writing and $c_2$ is used when reading, perhaps inspired by Reynolds [1997]. Unfortunately, the coercion-based implementation of gradual typing introduces overhead in the execution of statically-typed code. For example, a value of type $\text{ref int}$ may be simply an address or it may be an address wrapped in a coercion. Thus, every dereference must dispatch on the kind of value at run-time.

While efficiency is important, so is support for debugging. The casts used in gradual typing are related to *contracts*. The checking of higher-order contracts (involving functions or objects) happens in a delayed fashion, so an error may occur far away from the static location of the contract. Findler and Felleisen [2002] connect contract violations back to their static location using a technique now called *blame tracking*. Siek et al. [2009] adapt blame tracking to the Coercion Calculus, thereby improving error diagnostics in space-efficient implementations of gradual typing. However, the overhead in statically-typed code remains.

Wrigstad et al. [2010] remove this overhead by introducing a distinction between concrete types, for which there can be only one kind of value, and *like types*, for which there can be several kinds of values. However, their approach does not support blame tracking. Meanwhile, Siek and Wadler [2010] improve
Table 1. Summary of the gradual typing literature with respect to four properties.

<table>
<thead>
<tr>
<th>Efficient Casts</th>
<th>Blame Tracking</th>
<th>Fast Typed Code</th>
<th>Gradual State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Siek and Taha [2006]</td>
<td>○</td>
<td>○</td>
<td>●</td>
</tr>
<tr>
<td>Herman et al. [2007]</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Sick et al. [2009]</td>
<td>○</td>
<td>○</td>
<td>●</td>
</tr>
<tr>
<td>Wrigstad et al. [2010]</td>
<td>●</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>Sick and Wadler [2010]</td>
<td>●</td>
<td>○</td>
<td>●</td>
</tr>
</tbody>
</table>

The time efficiency of the coercion-based implementation by creating a succinct representation of coercions in normal form, called threesomes, together with an efficient algorithm for composing threesomes. Siek and Garcia [2012] adapt this algorithm to work directly on coercions.

Table 1 summarizes this prior work with respect to four properties: efficient casts, blame tracking, fast execution of statically-typed code, and supporting casts on values involving mutable state. The current situation is somewhat checkered; no prior design simultaneously supports all four properties. We give Herman et al. [2007] and Sick et al. [2009] a ○ on Efficient Casts because they do not define a time-efficient algorithm for coercion normalization. We give Sick and Taha [2006] ● on Gradual State because of the restrictive consistency rule discussed above. Wrigstad et al. [2010] get a ● on Gradual State because like types add complexity from the programmer’s viewpoint.

This paper presents two new designs to support gradual typing for mutable objects. These designs arose in the context of creating a gradually-typed version of Python but here we model the designs mathematically, creating two semantics for the imperative object calculus of Abadi and Cardelli [1996] extended with gradual typing. The first design, which we call guarded objects, is the natural extension of the coercion-based approach and thus still imposes overhead in statically-typed code. The second design, called monotonic objects, removes this overhead while still allowing casts on mutable objects and performing blame tracking. The key idea is that casts cause the run-time type of an object to become more statically typed. Table 2 summarizes our designs. We give monotonic objects a ● on Gradual State because it restricts objects to only become more statically typed.

Our presentation of guarded and monotonic objects is organized as follows. Section 2 describes in more depth the challenges that we face and gives an informal description of the new designs. Section 3 reviews gradual typing and introduces our gradually-typed imperative object calculus. Section 4 reviews the Coercion Calculus and develops object coercions. We define the semantics of guarded objects in Section 5 using an abstract machine to make explicit the costs in space and time. In Section 6 we adapt object coercions to the monotonic setting and define the abstract machine for monotonic objects. We discuss related work in Section 7 and Section 8 concludes.
2 Challenges of Gradual Typing with Mutable Objects

We begin with a review of gradual typing and discuss the challenges of adding gradual typing to languages with mutable objects. These challenges motivate our two designs, guarded and monotonic objects, which we introduce through examples written in a gradually-typed variant of Python.

2.1 Gradual Typing and Mutable State

To briefly review gradual typing, we begin with an example in which a dynamically-typed object is passed to the statically-typed `insert_to_db` function:

```python
class Person(object):
    def __init__(self, id, name):
        self.id = id
        self.name = name

    def insert_to_db(p : {id:int, name:str}) -> void:
        . . . p.name . . .

person1 = Person(1, 'John Doe')
insert_to_db(person1)
```

At the call to `insert_to_db`, the `person1` object is downcast from the dynamic type * (implicit in the source code) to the object type `{id:int, name:str}`. In this case the cast succeeds, but in general, such casts may fail. In the below example, `person2` has a unicode string in its `name` field, whose type is not consistent with `str`, so the implicit cast signals an error.

```python
person2 = Person(2, unicode('Pi'))
insert_to_db(person2) # Error, blame the implicit cast on this line
```

Next we consider an example in which gradual typing interacts in a problematic way with mutable state. (The problem is analogous to the classic problem of covariant subtyping for arrays.) Suppose that we create an alias to the dynamically-typed `person1` object with the `typed_person` variable. Then we mutate the `name` field of `person1` to a unicode string and finally call `insert_to_db`.

```python
typed_person : {id:int, name:str} = person1
person1.name = unicode(person1.name)
insert_to_db(typed_person)
```

The problem is that the type of the value in the `name` field has changed out from under the `typed_person` alias. In a na"ive implementation of gradual typing, when the statically-typed `insert_to_db` function accesses `p.name`, the result would be a unicode string instead of a string, which represents a hole in the type system. The following subsections present two different solutions to this problem: guarded objects and monotonic objects.
2.2 Guarded Objects

With guarded objects, each cast creates a guarded reference (a kind of proxy) to the underlying object. When fields are accessed through a guard, casts are applied to bridge the gap between the underlying type of the object and the type of the guard. In the problematic example, the implicit cast in the assignment to `typed_person` on line 13 creates a guard with type `{id:int, name:str}`. The subsequent assignment of a unicode string to the `name` field succeeds because the type of `person1.name` is `. Finally, the guarded reference is passed to `insert_to_db` which tries to access `p.name`. The guard handles this access by casting the unicode string to `str`, triggering a run-time error and blaming the cast on line 13. Thus, guarded objects close the hole in the type system by performing checks at every read and write to a member, analogous to how Java maintains type-safety despite the covariant subtyping of arrays. The idea of guarded objects is not novel [Strickland et al., 2012] but making them space-efficient is an open challenge that we address in Sections 4 and 5.

The main disadvantage of guarded objects is that some dispatching overhead occurs at every member access, even in statically-typed code. The following example sorts a list of persons by their id.

```python
def sort_persons_by_id(lst: list({id:int, name:str})) -> void:
  ... lst[i].id < lst[j].id ...
```

```python
person_list = [Person(1, 'John'), Person(2, 'Jane'), ...]
sort_persons_by_id(person_list)
```

Consider the task of separately compiling the `sort_persons_by_id` function. The compiler does not know whether the elements in `lst` will be guarded or unguarded and thus has to generate code that dispatches based on the kind of reference.

2.3 Monotonic Objects

The proxies used by guarded objects are needed because the values in an object’s fields may become inconsistent with the types of the guards. We can remove the overhead from fully-static field accesses (i.e., `*` does not appear in their static type) by ensuring that the runtime type of an object is no more dynamic than any reference to the object. Thus, if there is a fully-static reference, then the type of the field’s value must exactly match the type of the reference. To maintain this invariant, casts cause an object’s type to become more specific.

Turning back to the list sorting example, we see that the `person_list` is cast to `list({id:int, name:str})` at the call to `sort_persons_by_id`. Rather than wrapping the list in a proxy, as occurs with guarded objects, now the elements are cast to `{id:int, name:str}`. While casting all the elements of a list is a linear-time operation, any subsequent casts to the same list would be no-ops. So the worst-case overhead for the entire program is only a constant factor more than a cast-free execution of the program. Now consider the accesses to the `id` field inside the `sort_persons_by_id` function. The type of the field at this access is `int`, which is fully static, so by
our established invariant, the underlying value in the field must be an integer.
Thus, the field access can be compiled to overhead-free code. So with monotonic
objects, in regions of code that are fully static, we are able to achieve performance
comparable to that of a statically-typed language.

Next we discuss how to handle non-static (partially to fully dynamic) member
reads and writes and show where monotonic objects are more restrictive than
guarded objects. We return to the first example in which a dynamically typed
person is passed to the statically-typed insert_to_db function. However, this time
we read from id and write to name after the call to insert_to_db.

```python
21  def insert_to_db(p: {id: int, name: str}) → void:
22  ...
23  person = Person(1, 'John Doe')
24  insert_to_db(person)
25  print(person1.id)
26  person1.name = unicode(person1.name) # Error: blame cast on line 24
```

When the person is passed to insert_to_db, the underlying object is modified to
have type {id: int, name: str} by downcasting its members. But now we have a prob-
lem with the access to id after the call. The value in the id field is an integer,
but the type system expects it to have type *. This would be a problem for a
compiled implementation because integers would have different bit-level repre-
sentations than boxed values (values injected into *). We resolve this problem
by casting from int to * (boxing the integer) during the read. We emphasize that
such casts are only needed when the type of the field at the read site is partially
dynamic; if the type is fully-static, then no casts need to be performed.

Next we turn to the assignment of a unicode string to the name field of the
person1 object. In this case we cast the new value (a unicode string) from the
field’s static type (which is *) to the run-time type of the value in the field,
which is str. But this cast fails because the unicode string type is not consistent
with str, and the cast on line 24 is blamed. Thus, we see that while monotonic
objects are more efficient, they are also more restrictive than guarded objects.

Summary We have discussed two designs for gradually-typed, mutable objects.
Both approaches satisfy the fundamental goal of maintaining type safety in the
face of mutable state and something akin to covariant subtyping. However, the
characteristics and ideal use cases of each approach vary. The guarded objects
approach, by virtue of its ability to support strong updates (changes in the run-
time types), is appropriate for situations where the bulk of the program is written
in a highly dynamic style. The monotonic objects approach, on the other hand,
provides efficient field access in statically-typed code, which makes it ideal in sit-
uations where high performance is needed and where the intention of the devel-
oper is to migrate towards a fully-static program. The monotonic approach also
deals nicely with interoperability between languages such as Python and Java.
Jython (Python on the JVM [Hugunin et al., 1997]) currently uses an approach
similar to guarded objects but programmers complain of the overhead [Baker,
2012]. Using monotonic objects, this overhead could be removed.

In the rest of the paper, we develop mathematical models of both approaches.
3 Gradual typing and the imp₅λ*-calculus

Figure 1 defines the types of the imp₅λ*-calculus, which include the dynamic type ⋆ to support gradual typing and also some basic types (int and bool), function types, and object types of the form \([\Delta_1; \Delta_2]\). The \(\Delta_1\) maps a field’s label to the field’s type and \(\Delta_2\) maps a method’s label to its type.

Figure 1 also defines three relations on types: consistency, subtyping, and naive subtyping. The purpose of the the first two relations is to define which implicit conversions are allowed by the type system. Subtyping defines the safe up-casts, that is, conversions that never fail, whereas consistency allows any cast that might succeed. The naive subtyping relation captures the notion of how “dynamic” a type is, with ⋆ being the most dynamic type. The type ⋆ \(\rightarrow\) int is more dynamic than int \(\rightarrow\) int, so int \(\rightarrow\) int \(\leq_{n}\) ⋆ \(\rightarrow\) int even though these types are not in the subtype relation: int \(\rightarrow\) int \(\not\leq\) ⋆ \(\rightarrow\) int because ⋆ \(\not\leq\) int. The naive subtyping relation is used to express invariants of the dynamic semantics.

The subtyping relation on object types allows width subtyping but not depth subtyping for both fields and methods because both are mutable. The naive subtyping relation differs from subtyping because it allows depth subtyping on objects and because parameters of functions are covariant (instead of contravariant). The consistency relation is more permissive than subtyping, allowing widening and narrowing of an object, as well as variation in depth. The consistency relation just requires the common fields and methods to have consistent types. Unlike either subtyping relation, the consistency relation is symmetric, so it does
not make sense to talk about covariance versus contravariance. Additionally, the consistency relation is non-transitive.

Figure 2 defines the syntax and type system of the $\text{imp}_\lambda^{\star}$-calculus. This calculus includes some constants (Booleans and integers) and primitive operations, lambda expressions, let expressions, explicit casts, and objects with field and method projection and assignment. The calculus does not provide a special syntactic form for methods, but instead uses lambda expressions whose parameter is bound to the “self” argument during a method call. Method calls, which have the form $e \rightarrow l()$, are syntactic sugar for method projection plus self application. Multi-parameter methods can be simulated via currying.

The type system in Figure 2 includes the standard subsumption rule, so implicit up-casts are allowed according to the subtyping relation. The gradual nature of the type system can be seen in the rules that mention the dynamic type $\star$ and the consistency relation $\sim$. If an expression has type $\star$, then you can call it with an argument of any type. Also, you can project from and assign to any field or method of something of type $\star$.

The consistency relation is used where one might expect to see type equality. In a function application where the function has type $T_1 \rightarrow T_3$, the parameter type $T_2$ does not have to be equal to $T_1$, we just require $T_1 \sim T_2$. Except for subsumption, this type system is syntax directed, so it is straightforward to implement a type checking algorithm. (Siek and Taha [2007] describe an algorithm that handles subsumption in a gradual type system.)

As alluded to in the introduction, the dynamic semantics of a gradually-typed language is given by a translation to an intermediate language with explicit casts. For example, Ahmed et al. [2011] use the notation $e : T_1 \Rightarrow^\ell T_2$ for casting expression $e$ from its static type $T_1$ to $T_2$. The $\ell$ is the blame label that uniquely identifies the static location of the cast. In this paper we will use a variant of the Coercion Calculus to express casts and achieve space efficiency, so our notation for explicit casts in the intermediate language is $e : c$ where $c$ is a coercion. We discuss our addition of object coercions in the next section.

We use slightly different intermediate languages for guarded objects and monotonic objects. Both include explicit casts, but the intermediate language for monotonic objects includes a syntactic distinction between fast, statically-typed member projections versus dynamically-typed member projections. Thus, the intermediate language for guarded objects is defined in Section 5 and the intermediate language for monotonic objects is in Section 6.

4 Coercions for Mutable Objects

We begin with a review the Coercion Calculus and then develop object coercions.

The Coercion Calculus defines a set of instructions (or combinators) that tell a machine how to convert a value of one type to another type. Figure 3 defines the syntax of the Coercion Calculus extended with object coercions. The simplest coercion is the identity coercion, written $\iota$, which does not change the type of the coerced value. The injection coercion $I!$ converts from type $I$ to $\star$. One can
think of this coercion as “boxing” its input. The category \( I \) of injectable types includes all the types except \( * \). The evil twin of injection is projection, written \( I^\ell \), which converts from \( * \) to the type \( I \). This is a dangerous operation and might fail, in which case the blame goes to label \( \ell \). In the original Coercion Calculus, the injectable types did not include arbitrary function types, but only \( * \to * \).

The approach we take here, of including arbitrary function (and object) types in the injectables is a characteristic of the D blame tracking strategy of Siek et al. [2009]. The advantage of this approach is that safe casts are characterized by the subtyping relation that one would expect, that of Figure 1.

In some situations, to conserve space, we normalize coercions before it is time to apply them to a value. In such cases, we do not immediately signal an error, but instead just record it. This is the role of the \( \text{Fail} \) coercion [Herman et al., 2007]. The coercion \( c_1 \to c_2 \) is a function coercion, which applies \( c_1 \) to the argument of a function and \( c_2 \) to the return value. The sequence coercion \( c_1 ; c_2 \) applies \( c_1 \) and then \( c_2 \). (The standard notation for sequencing is \( c_2 \circ c_1 \), but we use the semicolon to carry on the improved left-to-right reading of casts.)

Fig. 2. The syntax and type system of the \( \text{imp}_\Gamma \lambda^* \)-calculus.
The type system for coercions is defined in Figure 3. We write \( \vdash c : T_1 \Rightarrow T_2 \) to say \( c \) is a well-typed coercion from source type \( T_1 \) to target \( T_2 \). Figure 3 also defines a partial function \( \langle T_1 \Rightarrow T_2 \rangle^\ell \) that creates a coercion from a source and target type and a blame label. This function is only defined when \( T_1 \sim T_2 \). When the source and target are subtypes, \( T_1 <: T_2 \), the resulting coercion contains no blame labels, so it is straightforward to see why such casts are safe.

4.1 Efficient Normalization of Coercions

The dynamic semantics of coercions is defined by a reduction semantics. However, there is a gap between such a semantics and an implementation. Following recent work of Siek and Garcia [2012], we define a composition operator, written \( c_1 \# c_2 \), that takes two coercions in normal form and produces the normal form for sequencing the two coercions (Figure 4). The composition operator is closely related to, but different from, the coercion sequence constructor \( c_1 ; c_2 \). The coercion \( c_1 ; c_2 \) normalizes to \( c_3 \) if and only if \( c_1 \# c_2 = c_3 \).

Let us consider some examples of how coercions work. Suppose the integer 42 is cast to dynamic. The resulting value has the form \( 42 : \text{int}! \). Next, suppose this value is cast back to \( \text{int} \), that is, it is projected using the coercion \( \text{int}?^\ell \). The semantics will compose the coercion on the value with the coercion of the cast. In this case, the result is the identity coercion: \( \text{int}! \# \text{int}?^\ell_1 = \langle \text{int} \Rightarrow \text{int} \rangle^\ell_1 = \iota \). Thus, the result of the cast back to \( \text{int} \) will simply be 42. On the other hand, if we cast to an inconsistent type, such as \( \text{bool} \), the result is a failure coercion which would then trigger a cast error: \( \text{int}! \# \text{bool}?^\ell_2 = \text{Fail}^\ell_2 \).

Our composition operator implements eager cast checking [Herman et al., 2007, Siek et al., 2009], which means that a cast failure is reported as soon as it is detected and applied to a value. With respect to the composition operator, this means that if the composition of any sub-coercion results in \( \text{Fail}^\ell \), then the overall result is \( \text{Fail}^\ell \). For example, the composition of the following two function coercions produces a failure because the composition of the codomain coercions produces a failure: \( (\iota \rightarrow \text{int}!) \# (\iota \rightarrow \text{bool}!^\ell_1) = \text{Fail}^\ell \) because \( \text{int}! \# \text{bool}?^\ell_2 = \text{Fail}^\ell \).

One of the subtle aspects of the Coercion Calculus is that coercion sequencing is associative and that all redexes are pairs of sequenced coercions. Thus, sometimes a sequence must be re-associated to reveal a redex. The last few lines of the definition of composition in Figure 4 deal with associativity by recursively invoking the composition operator. To ensure termination, we first check whether the coercion \( c_1 ; (c_2 ; c_3) \) is in normal form. This check is easy to perform because there are only two such normal forms: \( I^\ell; (\cdot \rightarrow \cdot); I! \) and the analogous form involving object coercions. The syntactic characterization of coercions in normal form is given at the bottom of Figure 4. The \textit{wrappers} \( \ell \), written \( \iota \), are coercions that may appear in a value. Also, the grammar for normal coercions relies on the auxiliary notion of a \textit{normal part}, which excludes failure coercions.
Syntax

blame labels $\ell \in B$
optional labels $p \in B^{opt}$ $::= \ell \mid \ell$
member coercions $f \in F ::= T^{opt}(c \leftrightarrow c)^p T^{opt}$
member maps $C \in L \rightarrow F$
injectables $I ::= B \mid T \rightarrow T \mid [\Delta; \Delta]$
coercions $c \in C ::= I \mid I^\ell \mid \text{Fail}^\ell$

$\vdash c : T \Rightarrow T$

$\vdash \iota : T \Rightarrow T$
$\vdash I! : I \Rightarrow \star$
$\vdash I^\ell! : \star \Rightarrow I$
$\vdash \text{Fail}^\ell : T_1 \Rightarrow T_2$

$\vdash c_1 : T_1 \Rightarrow T_1$
$\vdash c_2 : T_2 \Rightarrow T_2$
$\vdash c_1 ; c_2 : T_1 \Rightarrow T_1$

$\vdash c_1 : \Delta_1 \Rightarrow \Delta_3$
$\vdash c_2 : \Delta_2 \Rightarrow \Delta_4$
$\vdash [C_1; C_2] : [\Delta_1; \Delta_2] \Rightarrow [\Delta_3; \Delta_4]$

$\vdash C : \Delta \Rightarrow \Delta$

$\vdash C(l) : \Delta_1(l) \Rightarrow \Delta_2(l) \forall l \in \text{dom}(\Delta_1) \cap \text{dom}(\Delta_2)$
$\vdash C(l) : \Delta_1(l) \Rightarrow \epsilon \forall l \in \text{dom}(\Delta_1) - \text{dom}(\Delta_2)$
$\vdash C(l) : \epsilon \Rightarrow \Delta_2(l) \forall l \in \text{dom}(\Delta_2) - \text{dom}(\Delta_1)$
$\vdash C(l) : \epsilon \Rightarrow \epsilon \forall l \in \text{dom}(C) - \text{dom}(\Delta_1) - \text{dom}(\Delta_2)$

$\vdash C : \Delta_1 \Rightarrow \Delta_2$

$\vdash f : T^{opt} \Rightarrow T^{opt}$

$\vdash c_1 : T_2 \Rightarrow T_1$
$\vdash c_2 : T_1 \Rightarrow T_2$
$\vdash c_1 ; c_2 : T_1 \Rightarrow T_2$

$\vdash \epsilon(c_1 \leftrightarrow c_2)^\ell \epsilon : T_1 \Rightarrow T_2$
$\vdash \epsilon(c_1 \leftrightarrow c_2)^\ell T_2 : T_1 \Rightarrow \epsilon$
$\vdash \epsilon(c_1 \leftrightarrow c_2)^\ell \epsilon : T_1 \Rightarrow T_2$
$\vdash \epsilon(c_1 \leftrightarrow c_2)^\ell T_2 : T_1 \Rightarrow \epsilon$

$\vdash T \Rightarrow T^\ell$

$\langle B \Rightarrow B \rangle^\ell = \iota$
$\langle \epsilon \Rightarrow \epsilon \rangle^\ell = \iota$
$\langle I \Rightarrow I \rangle^\ell = I^\ell$
$\langle L \Rightarrow I \rangle^\ell = I^\ell$
$\langle T_1 \Rightarrow T_2 \Rightarrow T_3 \Rightarrow T_4 \rangle^\ell = \langle T_1 \Rightarrow T_3 \rangle^\ell \Rightarrow \langle T_2 \Rightarrow T_4 \rangle^\ell$
$\langle [\Delta_1; \Delta_2] \Rightarrow [\Delta_3; \Delta_4] \rangle^\ell = \langle [\Delta_1 \Rightarrow \Delta_3] ; \langle \Delta_2 \Rightarrow \Delta_4 \rangle \rangle^\ell$

$\langle \Delta \Rightarrow \Delta \rangle^\ell$

$\langle \Delta_1 \Rightarrow \Delta_2 \rangle^\ell (l) = \begin{cases} 
\epsilon(l) & \text{if } l \in \text{dom}(\Delta_1) \cap \text{dom}(\Delta_2) \\
\epsilon(l \leftrightarrow l)^\ell \epsilon(l) & \text{if } l \in \text{dom}(\Delta_1) - \text{dom}(\Delta_2) \\
\Delta_2(l) & \text{if } l \in \text{dom}(\Delta_2) - \text{dom}(\Delta_1)
\end{cases}$

$\overline{C}(l) = T_2^{opt}(c_2 \leftrightarrow c_1)^p T_1^{opt}$ where $C(l) = T_1^{opt}(c_1 \leftrightarrow c_2)^p T_2^{opt}$

Fig. 3. Coercions for mutable objects: syntax, type system, creation, and inversion.
\( I_1 \uparrow I_2 = \begin{cases} (I_1 \Rightarrow I_2) \uparrow & \text{if } I_1 \sim I_2 \\ \text{Fail} \uparrow & \text{otherwise} \end{cases} \)

\( (c_1 \rightarrow c_2) \uparrow (c_3 \rightarrow c_4) = \begin{cases} \text{Fail} \uparrow & \text{if } c_3 \uparrow c_1 = \text{Fail} \uparrow \\ \text{Fail} \uparrow & \text{if } c_2 \uparrow c_4 = \text{Fail} \uparrow \\ (c_3 \uparrow c_1) \rightarrow (c_2 \uparrow c_4) & \text{otherwise} \end{cases} \)

\([C_1; C_2] \uparrow [C_3; C_4] = \begin{cases} \text{Fail} \uparrow & \text{if } C_1 \uparrow C_3 = \text{Fail} \uparrow \\ \text{Fail} \uparrow & \text{if } C_2 \uparrow C_4 = \text{Fail} \uparrow \\ (C_1 \uparrow C_3; C_2 \uparrow C_4) & \text{otherwise} \end{cases} \)

\( \ell \uparrow c = c \uparrow \ell = c \)

\( c_1 \uparrow (c_2; c_3) = c_1 \uparrow (c_2 \uparrow c_3) \)

\( c_1 \uparrow c_2 = c_1 \uparrow c_2 \)

\( C \uparrow C \)

\( C_1 \uparrow C_2 = \begin{cases} C_3 & \text{if } \forall \ell \in \text{dom}(C_1) \cap \text{dom}(C_2), C_1(l) \uparrow C_2(l) \neq \text{Fail} \uparrow \\ \text{Fail} \uparrow & \text{if } C_1(l) \uparrow C_2(l) = \text{Fail} \uparrow \text{for some } \ell \end{cases} \)

where \( C_3(l) = \begin{cases} C_1(l) \cap C_2(l) & l \in \text{dom}(C_1) \cap \text{dom}(C_2) \\ C_1(l) & l \in \text{dom}(C_1) - \text{dom}(C_2) \\ C_2(l) & l \in \text{dom}(C_2) - \text{dom}(C_1) \end{cases} \)

\( f \uparrow f \)

\( T_4^{\text{opt}}(c_1 \leftarrow c_2)^\rho \uparrow (c_3 \leftarrow c_4)^\rho T_4^{\text{opt}} = \begin{cases} \text{Fail} \uparrow & \text{if } c_3 \uparrow c_1 = \text{Fail} \uparrow \\ \text{Fail} \uparrow & \text{if } c_2 \uparrow c_4 = \text{Fail} \uparrow \\ T_4^{\text{opt}}(c_3 \leftarrow c_2 \uparrow c_4)^\rho T_4^{\text{opt}} & \text{otherwise} \end{cases} \)

\( T_4^{\text{opt}}(c_1 \leftarrow c_2)^\eta T_2 \uparrow T_3(c_3 \leftarrow c_4)^\xi T_4^{\text{opt}} = \begin{cases} \text{Fail} \uparrow & \text{if } c_2 \uparrow c_4 = \text{Fail} \uparrow \\ \text{Fail} \uparrow & \text{if } c_0 \uparrow c_1 = \text{Fail} \uparrow \\ \text{Fail} \uparrow & \text{if } c_0 = \text{Fail} \uparrow \\ T_4^{\text{opt}}(c_3 \leftarrow c_2 \uparrow c_4) \uparrow T_4^{\text{opt}} & \text{otherwise} \end{cases} \)

where \( c_0 = c_3 \uparrow (T_3 \Rightarrow T_2)^\xi \uparrow c_1 \)

and \( c_0 = c_2 \uparrow (T_2 \Rightarrow T_3)^\xi \uparrow c_4 \)

\( p \uparrow p = p \)

\( \ell \uparrow q = \ell \)

\( \epsilon \uparrow q = q \)

**Normal forms**

wrappers \( \tau := I! | \tilde{c} \rightarrow \bar{c} | \tilde{\delta} \rightarrow \bar{\delta}; I! | [\tilde{C} ; \tilde{C}]; I! \)

normal parts \( \tilde{c} := \tau | \delta | I?^{\ell} | I?^{\xi}; \text{Fail}^{\ell} | I?^{\xi}; I! | I?^{\xi}; I! | I?^{\xi}; I! | I?^{\xi}; I! | [\tilde{C} ; \tilde{C}]; I! | [\tilde{C} ; \tilde{C}]; \text{Fail}^{\ell} | I?^{\xi}; [\tilde{C} ; \tilde{C}]; I! | [\tilde{C} ; \tilde{C}]; \text{Fail}^{\ell} | I?^{\xi}; [\tilde{C} ; \tilde{C}]; \text{Fail}^{\ell} \)

normal coercions \( \tilde{c} : c \rightarrow \tilde{c} \rightarrow \bar{c} \rightarrow \bar{\delta} \)

**Fig. 4.** Composition of coercions in normal form.
4.2 Object Coercions

An object coercion has the form $[C_1; C_2]$ and converts an object from one object type $[\Delta_1; \Delta_2]$ to another $[\Delta_3; \Delta_4]$. The $C_i$'s are partial functions from labels to member coercions, which require some explanation. Let us consider a few examples that motivate the general form of member coercions. First, suppose we wish to cast member $x$ from $\text{int}$ to $\ast$, that is, cast from $[x \mapsto \text{int}; \emptyset]$ to $[x \mapsto \ast; \emptyset]$. The object coercion might associate an injection $\text{int}!$ with field $x$. However, because fields are mutable, we need two coercions, one for writing and one for reading, just like reference coercions [Herman et al., 2007]. So in this example we would associate both $\text{int}?\ell$ and $\text{int}!$ with field $x$.

$$\vdash [x \mapsto (\text{int}?\ell \leftrightarrow \text{int}!); \emptyset] : [x \mapsto \text{int}; \emptyset] \Rightarrow [x \mapsto \ast; \emptyset]$$

We also want coercions that add or remove members. We prefix a member’s coercions with a type $T_1$ to indicate that we are adding a member of type $T_1$, and suffix the coercions with $T_2$ to indicate removal. Also, we may need a blame label to know which cast was responsible for the addition or removal. So the general form of a member coercion is $T_{\text{opt}}_1(c_1 \mapsto c_2)_{p} T_{\text{opt}}_2$, where $T_1$ and $T_2$ are optional types and $p$ is an optional blame label. The following two examples demonstrate coercions that add and remove field $x$.

$$\vdash [x \mapsto (\ell \mapsto \ell)_{\ell}; \emptyset] : [\emptyset; \emptyset] \Rightarrow [\ell \mapsto \text{int}; \emptyset]$$

$$\vdash [x \mapsto (\ell \mapsto \ell)_{\ell}\text{int}; \emptyset] : [\emptyset; \emptyset] \Rightarrow [\ell \mapsto \text{int}; \emptyset]$$

These prefixes and suffixes must be kept distinct from the member’s coercions so that we do not mistake member addition or removal with coercions on the member’s value. For example, the first of the following coercions converts the $x$ field from $\ast$ to $\text{int}$, whereas the second coercion adds field $x$.

$$\vdash [x \mapsto (\ell \mapsto \ell)_{\ell}; \emptyset] : [\ell; \emptyset] \Rightarrow [x \mapsto \text{int}; \emptyset]$$

$$\vdash [x \mapsto (\ell \mapsto \ell)_{\ell}\text{int}; \emptyset] : [\ell; \emptyset] \Rightarrow [x \mapsto \text{int}; \emptyset]$$

The type rule for object coercions, shown in Figure 3, takes four situations into account: the member is present in both the source and target type, only in one or the other, or in neither.

The composition of object coercions is defined in Figure 4. Similar to function coercions, if the composition of member coercions results in a failure, then the entire composition of object coercions results in failure. The composition of object coercions relies on the composition operator for member maps, $C_1 \triangleright C_2$. If a member $l$ is present in both $C_1$ and $C_2$, then we compose the two member coercions. Otherwise we just take the member coercion present in $C_1$ or $C_2$. The composition operator for member coercions, $f_1 \triangleright f_2$, must handle two cases, depending on whether $f_1$ performs member removal (and thus $f_2$ performs member addition), or not. In the case of a removal and addition, we bridge the gap between $T_2$ and $T_3$ by creating the coercions $T_2 \Rightarrow T_3)^{\ell_2}$ and $(T_3 \Rightarrow T_2)^{\ell_1}$. 13
expressions \( e \in \mathcal{E} := k \mid op(e) \mid \lambda x : T.e \mid e.c \mid [F; M] \mid e.l := e \mid e \rightarrow l := e \)

coercion expr. \( \hat{e} ::= x \mid \iota \mid I \ell \mid I! \mid \hat{\cdot}c \mid \hat{\cdot}c \rightarrow \hat{\cdot}c \mid [\hat{\cdot}C; \hat{\cdot}C] \mid \text{dom} \hat{\cdot}c \mid \text{cod} \hat{\cdot}c \)

statements \( s ::= x = e ; \mid x = e(e) ; \mid \text{return} e ; \mid \text{return} e(e) ; \mid \text{return} e(e) : \hat{\cdot}c ; \)

Fig. 5. Syntax of the intermediate language for guarded objects.

\[
\text{EvalMonad } A \equiv \text{Heap} \rightarrow (A \times \text{Heap}) + \{\text{blame}^\ell, \text{stuck}\}
\]

\[
x \leftarrow A; B \equiv \lambda \mu. \text{case } e \text{ of } \begin{cases} 
\text{return } v & \equiv \lambda \mu.(v, \mu) \\
\text{blame } \ell \Rightarrow \text{blame } \ell & \equiv \lambda \mu.(a, \mu(a := v)) \text{ if } a \notin \text{dom}(\mu) \\
\text{stuck} \Rightarrow \text{stuck} & \\
(v, \mu) \Rightarrow (\{x := v\}B)\mu & \equiv \lambda \mu.(a, \mu(a := v)) 
\end{cases}
\]

Fig. 6. The evaluation monad (EvalMonad).

5 Guarded Objects

With the development of coercions for objects complete, we are ready to present a space-efficient abstract machine for guarded objects. This machine operates on the intermediate language defined in Figure 5. The type system of this intermediate language is straightforward, so its definition is relegated to the Appendix.

The intermediate language is in a kind of A-normal form [Flanagan et al., 1993]. We separate function calls from the rest of the expressions, making calls into statements and storing their results in temporary variables. The last statement form \( \text{return } e(e) : \hat{\cdot}c ; \) is for function calls that would be tail calls except for an outstanding cast. One of the goals of this abstract machine is to make sure that such function calls are just as space efficient as if they were actually tail calls. The translation from the imp\(\lambda^\star\)-calculus to the intermediate language, which inserts casts and flattens function calls, only relies on standard techniques, so it is also given in the Appendix.

The definition of the abstract machine relies on an expression evaluation function \( [e] \rho \) (where \( \rho \) is an environment mapping variables to values) and a step function that executes one statement at a time, transitioning from one state to the next. Our machine must deal with abrupt termination due to cast errors and thread a global heap \( \mu \) through every computation, so to reduce syntactic clutter, we use the combination of a maybe monad and a state monad [Wadler, 1992]. This monad provides operators for sequencing computations, allocating on the heap, reading from the heap, and writing to the heap (Figure 6).

In Section 5.1 and 5.2 we describe expression evaluation and then the machine transitions, but first it is instructive to consider the values of the intermediate language, shown in Figure 7. The uncasted values (ranged over by \( \nu \)) include constants \( k \) and objects \([A_1; A_2]\), where \( A_1 \) gives the address for each field and \( A_2 \) gives the address for each method. An uncasted value may be wrapped in a
The definition of values for guarded objects.

Fig. 7. The definition of values for guarded objects.

uncasted values \( \nu \ ::= k \mid [A; A] \)  
values \( v \in V ::= \nu \mid \nu : \tau \mid (\lambda x y. \xi, \rho, \tau^{opt}) \)  
opt. coercions \( c^{opt} ::= \epsilon \mid c \)  
types \( T ::= \ldots \mid T_1 \Rightarrow T_2 \)  

Addresses \( a \in \mathbb{N} \)  
Member addresses \( A \in \mathbb{L} \rightarrow \mathbb{N} \)  
Environments \( \rho \in \mathbb{X} \rightarrow V \cup C \)  
Heaps \( \mu \in \mathbb{N} \rightarrow V \)

Lemma 1 (Canonical Forms for Guarded Objects).

1. If \( \Sigma \vdash v : B \), then \( v = k \) for some constant \( k \).
2. If \( \Sigma \vdash v : \tau \), then \( v \) has the forms \( \nu : \tau \) or \( \nu = (\lambda x y. \xi, \rho, \tau^{opt}) \), where the target type of \( \tau \) is \( \tau^{opt} \).
3. If \( \Sigma \vdash v : [\Delta_1; \Delta_2] \), then either \( v = [A_1; A_2] \) or \( v = [A_1; A_2] : [C_1; C_2] \).
4. If \( \Sigma \vdash v : T_1 \Rightarrow T_2 \), then \( v = (\lambda x y. \xi, \rho, \tau^{opt}) \).

The most important piece of the abstract machine is the \textit{cast} function, defined in Figure 8. This function takes a value and a coercion and returns a new value. The sixth equation is where we use coercion composition. The coercion \( c_2 \) is applied to a value already wrapped with \( c_1 \). We compose the two coercions and then call \textit{cast} on the result. (The result of the composition may be the identity or failure coercion.) The first three equations of the definition are straightforward: identity coercions are discarded and failure coercions raise blame. The fourth equation wraps an uncasted value in a cast. The fifth equation wraps an object with a coercion, but it must also check that the object has all of the fields required by the coercion, and if not, raise blame. We defer discussion of casting closures to Section 5.2.

5.1 Expression Evaluation for Guarded Objects

We define the evaluation of expressions in Figure 9. The case for casts, \( e : \hat{c} \) simply evaluates \( e \) and applies the \textit{cast} function. The cases for member projection and assignment are interesting because they reveal the run-time overhead inherent in guarded objects. In each we must dispatch between two cases, depending on whether the receiving object is just an object \( [A_1; A_2] \) or a casted object \( [A_1; A_2] : [C_1; C_2] \). The uncasted case is straightforward, performing a read or
cast(ν, ℓ) = ν

cast(ν, Failℓ) = blame ℓ

cast(ν, F) = blame ℓ

cast(ν, (c′; Failℓ)) = blame ℓ

if τ ≠ [C1; C2]

\[
\text{cast}(\nu, \tau) = \nu : \tau
\]

\[
\text{cast}(\nu : \tau) = \nu : \tau
\]

\[
\text{cast}(\nu : c_1, c_2) = \text{cast}(\nu, c_1 : c_2)
\]

\[
\text{cast}(\langle \lambda xy. s_1, \rho, \epsilon \rangle, c_2) = \text{return} \langle \lambda xy. s_1, \rho, \epsilon \rangle, c_2
\]

\[
\text{where } \tau_2 = \text{return } f(x : \text{dom}(y)) : \text{cod}(y);
\]

\[
\text{cast}(\langle \lambda xy. \tau, \rho, c_1 \rangle, c_2) = \begin{cases} 
\text{blame } \ell & \text{if } c_1 \Downarrow c_2 = \text{Fail}^\ell \\
& \text{or } c_1 \Downarrow c_2 = c \Downarrow \text{Fail}^\ell \\
\text{return} \langle \lambda xy. \tau, \rho, c_1 \Downarrow c_2 \rangle & \text{otherwise}
\end{cases}
\]

\[
\text{cast}(\langle \lambda xy. \tau_1, \rho, \epsilon \rangle, \tau_2) = \text{return} \langle \lambda xy. \tau_1, \rho, \epsilon \rangle, \tau_2
\]

\[
\text{if } \text{dom}(C_1) \subseteq \text{dom}(A_1)
\]

\[
\text{and } \text{dom}(C_2) \subseteq \text{dom}(A_2)
\]

\[
\text{if } C_i(l) = T_i(c_1 \mapsto c_2) \quad \text{if } l \notin \text{dom}(A_i), i \in \{1, 2\}
\]

\[
\text{cast}(\langle \lambda xy. \tau_1, \rho, \epsilon \rangle, \tau_2) = \text{return} \langle \lambda xy. \tau_1, \rho, \epsilon \rangle, \tau_2
\]

\[
\text{if } \text{dom}(C_1) \subseteq \text{dom}(A_1)
\]

\[
\text{and } \text{dom}(C_2) \subseteq \text{dom}(A_2)
\]

\[
\text{if } C_i(l) = T_i(c_1 \mapsto c_2) \quad \text{if } l \notin \text{dom}(A_i), i \in \{1, 2\}
\]

Fig. 8. The cast function for guarded objects.

write to the heap respectively for member projection or assignment. The case for a casted object is more subtle. For field projection, we read the value from the heap and then apply the \(c_2\) coercion. For method projection, we combine the \(c_2\) coercion with the inverse of the object coercion, \([C_1, C_2]\), to form a function coercion and apply that to the underlying closure. (The inversion operator is defined in Figure 3.) For field assignment, we apply the \(c_1\) coercion and for method updates, we combine the \(c_1\) coercion with the object coercion \([C_1, C_2]\) to form a function coercion that is applied to the closure.

### 5.2 Machine Transitions and Efficient Functions

We define the transitions of the abstract machine for guarded objects in Figure 10, in the form of the \texttt{step} function. The design of the \texttt{step} function makes function application efficient in both time and space. Regarding time, we do not want to dispatch on the kind of function values during a function call. Thus, we use a single value form for closures, shown in Figure 7, that contains a coercion and a flag to indicate whether the closure has ever been cast. When a closure is initially created, the coercion is absent (see the case for lambda expressions in Figure 9). The closure is given a second parameter \(y\), which will be bound to its optional coercion. However, the body \(\tau\) does not initially mention \(y\), so a closure that is never cast ignores its coercion. When a closure is cast for the first time, we generate a new closure and record the coercion. The new closure calls the original closure, but uses the \(y\) parameter to apply the recorded coercion to the argument and return value. To support this, we extend the language of coercions with variables and \texttt{dom} and \texttt{cod} operators, forming the syntactic category \(\hat{\cdot}\) (Figure 5).
\[ [\ell] \rho = \rho(x) \quad [x] \rho = \ell \quad [c_1 ; c_2] \rho = [[c_1] \rho ; [c_2] \rho] \quad \ldots \]

\[[e] : \text{EvalMonad} \mathcal{V} \]

\[ [k] \rho = \text{return } k \]
\[ [\text{op}(v)] \rho = v \leftarrow [[e] \rho; \text{return } \delta(\text{op}, v) \]
\[ [x] \rho = \text{return } \rho(x) \]
\[ [\lambda x. \pi] \rho = (\lambda x. \pi, \rho, \epsilon) \quad \text{y fresh} \]
\[ [[F; M]] \rho = v_1 \leftarrow [[e_1] \rho; a_1 \leftarrow \text{alloc}(v_1); \ldots \text{return } \{ l_i = a_i \quad i = 1 \ldots n ; l_j = a_j \quad i = n + 1 \ldots m \} \]
where \( F = \{ l_1 \mapsto e_1, \ldots, l_n \mapsto e_n \} \) and \( M = \{ l_{n+1} \mapsto e_{n+1}, \ldots, l_m \mapsto e_m \} \)
\[ [[c. l]] \rho = v \leftarrow [[e] \rho; \]
\[ \begin{cases} \text{read}(A_1(l)) & \text{if } v = [A_1 ; A_2] \\ v' \leftarrow \text{read}(A_1(l)); \text{cast}(v', c_2) & \text{if } v = [A_1 ; A_2] : [C_1 ; C_2] \text{ and } C_1(l) = T_1^{\text{opt}}(c_1 \leftarrow c_2)^p T_2^{\text{opt}} \end{cases} \]
\[ [[e \rightarrow l]] \rho = v \leftarrow [[e] \rho; \]
\[ \begin{cases} \text{read}(A_2(l)) & \text{if } v = [A_1 ; A_2] \\ v' \leftarrow \text{read}(A_1(l)); \text{cast}(v', \{ C_1 ; C_2 \} \rightarrow c_2) & \text{if } v = [A_1 ; A_2] : [C_1 ; C_2] \text{ and } C_2(l) = T_1^{\text{opt}}(c_1 \leftarrow c_2)^p T_2^{\text{opt}} \end{cases} \]
\[ [[c_1 . l := e_2]] \rho = v_1 \leftarrow [[e_1] \rho ; v_2 \leftarrow [[e_2] \rho; \]
\[ \begin{cases} \_ \leftarrow \text{write}(A_1(l), v_2); \text{return } [A_1 ; A_2] & \text{if } v_1 = [A_1 ; A_2] \\ v'_2 \leftarrow \text{cast}(v_2, c_1); _\leftarrow \text{write}(A_1(l), v'_2) & \text{if } v_1 = [A_1 ; A_2] : [C_1 ; C_2] \text{ and } C_1(l) = T_1^{\text{opt}}(c_1 \leftarrow c_2)^p T_2^{\text{opt}} \end{cases} \]
\[ [[e_1 \rightarrow l := e_2]] \rho = v_1 \leftarrow [[c_1] \rho ; v_2 \leftarrow [[e_2] \rho; \]
\[ \begin{cases} \_ \leftarrow \text{write}(A_2(l), v_2); \text{return } [A_1 ; A_2] & \text{if } v_1 = [A_1 ; A_2] \\ v'_2 \leftarrow \text{cast}(v_2, [C_1 ; C_2] \rightarrow c_1) & \text{if } v_1 = [A_1 ; A_2] : [C_1 ; C_2] \text{ and } C_2(l) = T_1^{\text{opt}}(c_1 \leftarrow c_2)^p T_2^{\text{opt}} \end{cases} \]
\[ [[e : \_] \rho = v \leftarrow [[e] \rho; \text{cast}(v, [\_] \rho) \]

Fig. 9. Expression evaluation for guarded objects.
stacks \( \kappa ::= c \cdot K \) \quad K ::= \epsilon \mid (x, \pi, \rho) \cdot \kappa \quad \text{states} \quad \sigma ::= (\pi, \rho, \kappa)

\textbf{step} : \text{State} \to \text{EvalMonad State}

\begin{align*}
\text{step} \langle x = e; \pi, \rho, \kappa \rangle &= v \leftarrow [e] \rho; \text{return} \ (\pi, \rho(x:=v), \kappa) \\
\text{step} \langle x = e_1(e_2); \pi_1, \rho_1, \kappa \rangle &= \langle \lambda y \ z. \pi_2, \rho_2, c \rangle \leftarrow [e_1] \rho; v_2 \leftarrow [e_2] \rho; \\
&\quad \text{return} \ (\pi_2, \rho_2(y:=v_2)(z:=c), c \cdot (x, \pi_1, \rho_1) \cdot \kappa) \\
\text{step} \langle \text{return} \ e_1; \rho_1, c \cdot (x, \pi, \rho_2) \cdot \kappa \rangle &= v \leftarrow [e_1] \rho; v' \leftarrow \text{cast}(v, c); \text{return} \ (\pi, \rho_2(x:=v'), \kappa) \\
\text{step} \langle \text{return} \ e_1(e_2); \rho_1, c_1 \cdot K \rangle &= \langle \lambda y \ z. \pi_2, \rho_2, c_1 \rangle \leftarrow [e_1] \rho; v_2 \leftarrow [e_2] \rho; \\
&\quad \text{return} \ (\pi_2, \rho_2(y:=v_2)(z:=c_1), c_2 \cdot K) \\
\text{step} \sigma &= \text{stuck} \quad \text{if none of the above apply}
\end{align*}

\textbf{step}^* : \text{State} \to \text{EvalMonad State}

\begin{align*}
\text{step}^* \sigma &= \begin{cases} 
\sigma & \text{if } \sigma = \langle \text{return} \ e_1; \rho, c \cdot \epsilon \rangle \\
\sigma' \leftarrow \text{step} \sigma; \text{step}^* \sigma' & \text{otherwise}
\end{cases}
\end{align*}

\textbf{Fig. 10.} The \textit{step} and eval functions for guarded objects.

Turning our attention to the second equation of \textit{step} in Figure 10, we see the transition for function calls. In addition to passing the normal argument \( v_2 \), we also pass the function’s coercion \( c \). Thus, we push the responsibility of performing the cast from the caller to the callee, thereby removing caller-side overhead. Furthermore, if the callee was never cast, then it ignores the coercion parameter, so there is no overhead on the callee side either. It would be nice if we could apply the same trick for member projection but functions provide a layer of indirection that is not present in objects.

The design of the \textit{step} function also addresses space efficiency for tail calls. On a tail call (the fourth and fifth equations), we do not push a new procedure call frame. To prevent the build-up of coercions, for the tail call and cast combination, we take the outstanding coercion \( \dot{c}_2 \) and compose it with the coercion \( c_3 \) at the top of the stack. The coercions stored on the stack come into play upon return from a function call: we apply the coercion to the return value.

5.3 The Dynamic Semantics of Guarded Objects

To conclude our treatment of guarded objects, Figure 11 defines the dynamic semantics on the \textit{imp}_{\text{Cf}}\textit{\lambda}^{+} -calculus as the \textit{eval} function, which maps a source program to an observable. In other words, an implementation of the \textit{imp}_{\text{Cf}}\textit{\lambda}^{+} -calculus is only required to produce the same observable as \textit{eval}. The \textit{eval} function
\[
\text{eval}(e) = \begin{cases} 
\text{observe}(v') & \text{if step}^* \sigma_0 \mu_0 = ((\text{return } e; \rho, c \cdot \epsilon), \mu_1), \\
\text{blame } \ell & \text{if step}^* \sigma_0 \mu_0 = \text{blame } \ell \\
\text{stuck} & \text{if step}^* \sigma_0 \mu_0 = \text{stuck}
\end{cases}
\]

where \( \emptyset \vdash e : T \) and \( \emptyset ; T \vdash e \sim \pi \) and \( \sigma_0 = (\pi, \emptyset, l \cdot \epsilon) \) and \( \mu_0 = \emptyset \)

\[
\begin{align*}
\text{observe}(k) &= k \\
\text{observe}([A_1; A_2]) &= \text{observe}([A_1; A_2] : [C_1; C_2]) = \text{object} \\
\text{observe}(\nu : I!) &= \text{observe}(\nu : (c; I!)) = \text{dynamic} \\
\text{observe}((\lambda x y. \pi, \rho, c, b)) &= \text{function}
\end{align*}
\]

Fig. 11. The dynamic semantics of guarded objects, defined as the eval function.

applies the cast insertion translation to convert \( e \) to a sequence of statements \( \pi \), and then applies the step* function. If the program terminates normally, the observe function is applied to the value.

6 Monotonic Objects

The primary design goal for monotonic objects is to remove the overhead that we saw in guarded objects regarding member projection and assignment. To accomplish this we need the following property: if an expression is of object type, then the resulting value must be an actual object and not a guarded object. However, we still want to allow convenient interaction between static and dynamic code, for example, an object of type \( [x \mapsto \star; \emptyset] \) can be passed into a function expecting \( [x \mapsto \text{int}; \emptyset] \). Our solution is to change the object during the cast: we check that the value stored in \( x \) is an integer and then unbox it.

The overall invariant that we maintain is that the type \( T_1 \) of the value at address \( a \) in the heap is equal to or less dynamic than (a naive subtype of) the type \( T_2 \) of any reference to \( a \), so \( T_1 \lesssim_n T_2 \). Thus, if we have an object \( [x \mapsto a; \emptyset] \) of type \( [x \mapsto \text{int}; \emptyset] \), then \( T_1 \lesssim_n \text{int} \) and so \( T_1 = \text{int} \). So the value at address \( a \) must be an integer and the implementation can read it with zero run-time overhead. We use the name monotonic objects because the type of a value in the heap is allowed to monotonically decrease with respect to naive subtyping.

The intermediate language for monotonic objects, shown in Figure 12, differs slightly from that of guarded objects. The abstract machine needs the static type of an object at object creation, so we record its type in the syntax for object creation. Also, we distinguish between field projections in which the type of the field is fully static (\( \star \) does not appear in the type) or not. We write a fully static field projection as normal, \( e.l \), whereas a non-static projection is annotated with the static type of the field, \( e.l_T \). We give the same treatment
expressions  
\[ e \in E ::= k \mid \text{op}(e) \mid x \mid \lambda x : T. e \mid e : \ell \mid [F; M] \text{as} \ [\Delta; \Delta] \mid e.1 \mid e.eT ::= e \mid e.lT ::= e \mid e\rightarrow l \mid e\rightarrow lT \mid e\rightarrow l ::= e \mid e\rightarrow lT ::= e \]

statements  
\[ s ::= \text{same as for guarded objects} \]

uncasted values  
\[ \nu ::= k \mid [A; A] \]

values  
\[ v \in V ::= \nu \mid \nu : ! \mid \langle \lambda x. \bar{s}, \rho, \bar{c} \rangle \]

labeled types  
\[ L \in T^\ell ::= B^p \mid * \mid [A; A]^p \mid L \rightarrow^p L \]

labeled type map  
\[ A \in L \rightarrow T^\ell \times B^\text{opt} \]

heaps  
\[ \mu \in N \rightarrow V \times T^\ell \]

Fig. 12. The intermediate language and values for monotonic objects.

to field assignment and method access. The type system for this intermediate language is straightforward so its definition is in the Appendix, Figure 20.

Before describing expression evaluation, let us study the forms of values, defined in Figure 12. As before, we have constants, objects, and closures. However, we no longer have casted objects. We also make a change to the heap by storing a labeled type with each value. This type is the type of the value but annotated with blame labels that say which casts were responsible for each part of the type.

The typing rules for values are in the Appendix, Figure 24.

**Lemma 2 (Canonical Forms for Monotonic Objects).**

1. If \( \Sigma \vdash v : B \), then \( v = k \) for some constant \( k \).
2. If \( \Sigma \vdash v : * \), then \( v \) has the form \( v = \nu : ! \) or \( v = \langle \lambda x. \bar{s}, \rho, \bar{c} \rangle \), where the target type of \( \bar{c} \) is \( * \).
3. If \( \Sigma \vdash v : [\Delta_1; \Delta_2] \), then \( v = [A_1; A_2] \).
4. If \( \Sigma \vdash v : T_1 \rightarrow T_2 \), then \( v = \langle \lambda x. \bar{s}, \rho, \bar{c}^\text{opt} \rangle \).

Figure 13 defines expression evaluation for monotonic objects. The equations for constants, primitive operations, variables, and lambda expressions are the same as those for guarded objects. For object creation, the only change is that the type of each member is stored next to the value in the heap.

The evaluation rules for non-static member access are subtle. The reference’s type for a member, \( T \), may be be more dynamic than the corresponding value in the heap. Thus, when projecting a member we must cast the value from its labeled type \( L \) to \( T \). We use the notation \( L \Rightarrow T \) for the operator that constructs a coercion from \( [L] \) to \( T \) and give its definition in Figure 13. (The operator \([L]\) erases the labels from a labeled type; see Figure 23 in the Appendix.) Conversely, when assigning to a member, we must cast from \( T \) to \( L \). Figure 13 also define the operator \( T \Rightarrow L \). The definitions of these two operators are mutually recursive because of the contravariance in function types. Because \([L] \prec_n T\), the operator \( L \Rightarrow T \) primarily produces identity coercions and injections, whereas \( T \Rightarrow L \).
\[
\begin{align*}
[[F; M] &\Rightarrow [\Delta_1; \Delta_2]] = \langle v_1 \leftarrow [e_1]p; a_1 \leftarrow \text{alloc}(\langle v_1, [\Delta_1(l_1)] \rangle) \rangle; \\
&\cdots \\
v_{n+1} &\leftarrow [e_{n+1}]p; a_{n+1} \leftarrow \text{alloc}(\langle v_{n+1}, [\Delta_1; \Delta_2] \Rightarrow \Delta_2(l_{n+1}) \rangle) ; \\
&\cdots \\
\text{return } [l_i = a_i, i=1..n; l_j = a_j, j=n+1..m] \\
\text{where } F = \{ l_1 \rightarrow e_1, \ldots, l_n \rightarrow e_n \} \text{ and } M = \{ l_{n+1} \rightarrow e_{n+1}, \ldots, l_m \rightarrow e_m \} \\
\end{align*}
\]

\[\begin{align*}
[e.]p &\Rightarrow [A_1; A_2] \leftarrow [e]p; (v, L) \leftarrow \text{read}(A_1(l)); \text{return } v \\
\langle e \rightarrow l \rangle.p &\Rightarrow [A_1; A_2] \leftarrow [e]p; (v, L) \leftarrow \text{read}(A_2(l)); \text{return } v \\
[e_1, l := e_2].p &\Rightarrow [A_1; A_2] \leftarrow [e_1].p; v_2 \leftarrow [e_2].p; \\
(\_L) &\leftarrow \text{read}(A_1(l)); \_L &\leftarrow \text{write}(A_1(l), (v_2, L)); \text{return } [A_1; A_2] \\
[e_1 \rightarrow l := e_2].p &\Rightarrow [A_1; A_2] \leftarrow [e_1].p; v_2 \leftarrow [e_2].p; \\
(\_L) &\leftarrow \text{read}(A_2(l)); \_L &\leftarrow \text{write}(A_2(l), (v_2, L)); \text{return } [A_1; A_2] \\
\end{align*}\]

\[\begin{align*}
T &\Rightarrow c \text{ precondition: } [L] .<_{\Delta_1} T, \text{ postcondition: } \vdash c : [L] \Rightarrow T \\
B^p &\Rightarrow B = \ell \quad * \Rightarrow * = \ell \\
\vdash [A_1; A_2]^p \Rightarrow [\Delta_3; \Delta_1] = [A_1 \Rightarrow \Delta_3; A_2 \Rightarrow \Delta_4] \\
L_1 \rightarrow^p L_2 \Rightarrow T_3 \rightarrow T_4 = (T_3 \Rightarrow L_1) \rightarrow (L_2 \Rightarrow T_4) \\
\end{align*}\]

\[\begin{align*}
A &\Rightarrow \Delta = A \text{ precondition: } [A] .<_{\Delta_1} \Delta \\
(A \Rightarrow \Delta)(l) &\Rightarrow \begin{cases} 
(A(l)_1 \Rightarrow \Delta(l), \epsilon) & \text{ if } l \in \text{dom}(\Delta) \\
(A(l)_1 \Rightarrow \Delta(l), A(l)_2) & \text{ if } l \notin \text{dom}(\Delta) 
\end{cases} \\
T &\Rightarrow [L] . c \text{ precondition: } [L] .<_{\Delta_1} T, \text{ postcondition: } \vdash c : T \Rightarrow [L] \\
B &\Rightarrow B^p = \ell \quad * \Rightarrow * = \ell \\
* \Rightarrow L = [L]^\ell \text{ where } \ell = \text{toLabel}(L) \text{ and } L \neq * \\
[\Delta_1; \Delta_2] &\Rightarrow [A_3; A_4]^p = [\Delta_1 \Rightarrow A_3; \Delta_3 \Rightarrow A_4] \\
T_1 \rightarrow T_2 \Rightarrow L_3 \rightarrow^p L_4 = (L_3 \Rightarrow T_1) \rightarrow (T_2 \Rightarrow L_4) \\
\end{align*}\]

\[\begin{align*}
\Delta &\Rightarrow A = A \text{ precondition: } [A] .<_{\Delta_1} \Delta \\
(\Delta \Rightarrow A)(l) &\Rightarrow \begin{cases} 
(\Delta(l) \Rightarrow A(l)_1, \epsilon) & \text{ if } l \in \text{dom}(\Delta) \\
(\Delta(l) \Rightarrow A(l)_1, A(l)_2) & \text{ if } l \notin \text{dom}(\Delta) 
\end{cases} \\
\end{align*}\]

Fig. 13. Expression evaluation for monotonic objects and auxiliary definitions.
produces identities and projections. The auxiliary toplabel function just returns the top-most label in the type, and is defined in Figure 23 of the Appendix.

The last equation of Figure 13 looks the same as in guarded objects, but it is really quite different because the cast function behaves differently. The cast function must maintain the invariant that the values on the heap are less or equally dynamic than any reference to them. In particular, we may need to unbox some values (or signal a cast error) to make the value’s type as static as the target type of the cast.

The notion of an object coercion is different with the monotonic approach because the act of casting an object does not build a new reference to the object, it changes the object’s representation in the heap. Figure 14 defines coercions for monotonic objects. The syntax of an object coercion now uses labeled type maps instead of member coercion maps: \([A_1; A_2]\) instead of \([C_1; C_2]\). The idea is that an object coercion changes an object so that its fields and methods are no more dynamic than the labeled types specified by \(A_1\) and \(A_2\), respectively.

With this change, the algorithm for composing two object coercions needs to be updated. We define what composition means for the labeled type maps and also for labeled types in Figure 14. The composition of labeled types computes the greatest lower bound with respect to naive subtyping (if it exists). A greatest lower bound exists if and only if the two types are consistent, that is, \(L_1 \uparrow L_2 \neq \text{Fail}\) if and only if \(\lfloor L_1 \rfloor \sim \lfloor L_2 \rfloor\). The composition operator can be viewed as an eager variant of the composition operator defined by Siek and Wadler [2010].

Figure 15 defines the cast function for monotonic objects. The equations are essentially the same as before except for objects. When casting an object, we invoke the auxiliary Cast function to coerce the object’s fields and methods and then return the object. For each member \(l_i\), the Cast function reads its value \(v_i\) and labeled type \(L_i\), then composes \(L_i\) with the labeled type in the cast, \(A(l_i)\) to get the new labeled type \(L'_i\) for the member. Then the member’s value \(v_i\) is cast to \(L'_i\), making use of the auxiliary operator \(L_i \sim L'_i\), defined in Figure 15. Finally, the new value is written back into the field.

The treatment of functions and function calls in monotonic objects is the same as for guarded objects. Thus, the step function for guarded objects can be adapted by simply replacing the expression and coercion evaluation functions and the cast function. The eval function can be similarly adapted with some minor changes to the observe function to handle the changes in the value forms. Thus, our formal description of monotonic objects is complete.

7 Related Work

Our work on monotonic objects was partly inspired by analogous work on type-state systems. Fähndrich and Leino [2003] introduce the notion of monotonic typestate, in which an object may proceed from less restrictive to more restrictive typestates, but not vice versa. Our work differs in that the monotonicity is enforced by a combination of static and dynamic checking (which is necessary for dealing with dynamically-typed regions of code) whereas with monotonic
coercions $c \in C ::= \iota \mid I \mid I \Rightarrow \iota \mid \text{Fail} \mid c \cdot c \rightarrow c \mid [A; A]$

$$(\Delta \Rightarrow \Delta)^\ell$$

$$(\Delta_1 \Rightarrow \Delta_2)^\ell(l) = \begin{cases} (\Delta_1(l))^\ell \Rightarrow (\Delta_2(l))^\ell, \epsilon & \text{if } l \in \text{dom}(\Delta_1) \cap \text{dom}(\Delta_2) \\ (\Delta_1(l))^\ell, \ell & \text{if } l \in \text{dom}(\Delta_1) - \text{dom}(\Delta_2) \\ (\Delta_2(l))^\ell, \ell & \text{if } l \in \text{dom}(\Delta_2) - \text{dom}(\Delta_1) \end{cases}$$

$$c \triangleleft c$$

... (1)

$$[A_1; A_2] \triangleleft [A_3; A_4] = \begin{cases} \text{Fail}^\ell & \text{if } A_1 \triangleleft A_3 = \text{Fail}^\ell \\ \text{Fail}^\ell & \text{if } A_2 \triangleleft A_4 = \text{Fail}^\ell \\ [A_1 \triangleleft A_3; A_2 \triangleleft A_4] \text{ otherwise} \end{cases}$$

$L_1 \triangleleft L_2 = L_3$ or $\text{Fail}^\ell$

postcondition: $[L_3] <_n [L_1], [L_3] <_n [L_2]$

$$* \triangleleft L = L$$

$$L \triangleleft * = L$$

$$B^p \triangleleft B^q = B^{p|q}$$

$$L_1 \rightarrow^p L_2 \triangleleft L_3 \rightarrow^q L_4 = \begin{cases} \text{Fail}^\ell & \text{if } L_3 \triangleleft L_1 = \text{Fail}^\ell \\ \text{Fail}^\ell & \text{if } L_2 \triangleleft L_4 = \text{Fail}^\ell \\ (L_3 \triangleleft L_1) \rightarrow^p \triangleleft (L_2 \triangleleft L_4) \text{ otherwise} \end{cases}$$

$$[A_1; A_2]^p \triangleleft [A_3; A_4]^q = \begin{cases} \text{Fail}^\ell & \text{if } A_1 \triangleleft A_3 = \text{Fail}^\ell \\ \text{Fail}^\ell & \text{if } A_2 \triangleleft A_4 = \text{Fail}^\ell \\ [A_1 \triangleleft A_3; A_2 \triangleleft A_4]^{p|q} \text{ otherwise} \end{cases}$$

$L_1 \triangleleft L_2 = \text{Fail}^\ell$ if $\text{head}(L_1) \neq \text{head}(L_2)$ and $\text{toplabel}(L_2) = \ell$

$$\text{head}(B^p) = B \quad \text{head}([A_1; A_2]^p) = \text{object} \quad \text{head}(L_1 \rightarrow^p L_2) = \text{function}$$

$$A \triangleleft A = A$$

$$A_1 \triangleleft A_2 = \begin{cases} \text{Fail}^\ell & \text{if } A_1(l) \triangleleft A_2(l) = \text{Fail}^\ell \text{ for some } l \\ A_3 \text{ otherwise} \end{cases}$$

where $A_3(l) = \begin{cases} A_1(l) \triangleleft A_2(l) & \text{if } l \in \text{dom}(A_1) \cap \text{dom}(A_2) \\ A_1(l) & \text{if } l \in \text{dom}(A_1) - \text{dom}(A_2) \\ A_2(l) & \text{if } l \in \text{dom}(A_2) - \text{dom}(A_1) \end{cases}$

$$(L, p) \triangleleft (L, p) = (L, p)$$

$$(L_1, p) \triangleleft (L_2, q) = \begin{cases} \text{Fail}^\ell & \text{if } L_1 \triangleleft L_2 = \text{Fail}^\ell \\ (L_1 \triangleleft L_2, p \triangleleft q) \text{ otherwise} \end{cases}$$

Fig. 14. Coercions for monotonic objects and composition of labeled types.
\[
\text{cast}([A_1; A_2], [A_1; A_2]) = _\ast \leftarrow \text{Cast}(A_1, A_1) ; _\ast \leftarrow \text{Cast}(A_2, A_2) ; \text{return} [A_1; A_2]
\]

\[
\text{Cast}(A, A) = \begin{cases} 
\text{blame } A(l_2) & \text{if } \exists l \in \text{dom}(A) \text{ and } l \notin \text{dom}(A) \\
(v_1, l_1) \leftarrow \text{read}(A(l_1)); \\
L_1' \leftarrow L_1 \uplus A(l_1); \\
v_1' \leftarrow \text{cast}(v_1, c); \\
_\ast \leftarrow \text{write}(A(l_1), (v_1', L_1')); \cdots 
\end{cases}
\]

\[
L_1 \sim L_2 \iff c\quad \text{precondition: } [L_2] \prec_{\sim_n} [L_1]
\]

\[
B^p \sim B^q = \ast \quad \ast \sim \ast = \ast \quad \ast \sim L = [L]^? \ell \quad (\text{where } \ell = \text{toplabel}(L) \text{ and } L \neq \ast)
\]

\[
[A_1; A_2]^p \sim [A_3; A_4]^q = [A_3; A_4] \quad L_1 \rightarrow^p L_2 \sim L_3 \rightarrow^q L_4 = (L_3 \sim L_1) \rightarrow (L_2 \sim L_4)
\]

**Fig. 15.** The `cast` function and auxiliary definitions.

typtstate, the monotonicity is enforced statically. Jagadeesan et al. [2009] adapt monotonic typtstate to the impς-calculus [Abadi and Cardelli, 1996].

The work on gradual typtstate by Wolff et al. [2011] is related to ours in that typtstate checking occurs both statically and dynamically. However, their system does not rely on monotonicity but instead uses reference counting.

The work on Typed Scheme and Racket [Tobin-Hochstadt and Felleisen, 2006, 2008, Takikawa et al., 2012, Strickland et al., 2012] falls into the same category as our guarded objects, in that values are wrapped with guards. The Racket implementation is a just-in-time compiler and its handling of guards imposes no more overhead than its handling of dynamic typting. In our system, there is no overhead in statically-typed code. The Racket implementation does not address space efficiency.

8 Conclusion

The design and implementation of gradually-typed languages with mutable objects is challenging. It is difficult to ensure type safety while also enabling fast execution of statically-typed code. This paper presents the first design, named monotonic objects, that does both. This design is especially suitable in situations that require high performance in parts of an application and where the intention of the programmer is to eventually migrate the entire program to static typting.

This paper also develops an alternative approach, guarded objects, that is the natural extension of earlier coercion-based implementations of gradual typting. Guarded objects induce some overhead in statically-typed code, but they are less restrictive than monotonic objects and are therefore more suitable in situations where the bulk of the program is written in a highly dynamic style.
Acknowledgments

We thank Carl Friedrich Bolz and Ronald Garcia for helpful discussions about this research. This research was funded by NSF award 0846121.
Bibliography


Appendix

This appendix supplies additional definitions concerning the semantics of guarded and monotonic objects.

Guarded objects

We describe the type system of guarded objects and their coercions in Figure 16. This figure extends the type system of the $\textbf{imp}_{\lambda}^{\text{⋆}}$-calculus, as shown in Figure 2, and the type system of object coercions, as shown in Figure 3. It also defines the type system for statements in the intermediate language for guarded objects.

The coercion inserting translation from the $\textbf{imp}_{\lambda}^{\text{⋆}}$-calculus to the intermediate language for guarded objects is shown in Figures 17 and 18.

Figure 19 contains the value and store typing judgments for guarded objects.

Monotonic objects

Figure 20 defines the type system for the intermediate language of monotonic objects. It extends the type system of guarded objects, in Figure 16, and likewise inherits from Figures 2 and 3.

Figure 21 extends and overrides Figures 17 and 18 to define the coercion inserting translation from the $\textbf{imp}_{\lambda}^{\text{⋆}}$-calculus to the intermediate language for monotonic objects. Figure 22 shows the judgment that determines whether or not a type is fully-static (lacking $\text{⋆}$), and therefore whether or not member accesses and writes to a field or method can be direct.

Figure 23 specifies several straightforward utility functions used during the casting process of monotonic objects. The $\text{toplabel}$ function returns the outermost blame label (if one exists) of a labeled type. The $\lfloor L \rfloor$ function erases the labels from a labeled type to acquire a normal type, and the $\lceil T \rceil^p$ function applies a blame label to a normal type to create a labeled type.

Figure 24 contains the value and store typing judgments for monotonic objects.
Fig. 16. The type system for the intermediate language of guarded objects.
Fig. 17. Coercion insertion and conversion to ANF for guarded objects, part 1.
\[ \Gamma \vdash \llbracket e \rrbracket \sim \llbracket s \rrbracket : T \]

<table>
<thead>
<tr>
<th>( e \neq e'_1 e'_2 )</th>
<th>( e \neq e'_1 : T )</th>
<th>( \Gamma \vdash \llbracket e \rrbracket \sim \llbracket s \rrbracket, \llbracket e'_1 \rrbracket : T_1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \Gamma \vdash \llbracket e \rrbracket \sim \llbracket s \rrbracket : T_1 )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \Gamma \vdash \llbracket e_2 \rrbracket \sim \llbracket s_1 \rrbracket, \llbracket e'_2 \rrbracket : T_1 \rightarrow T_2 )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \Gamma \vdash \llbracket e_2 \rrbracket \sim \llbracket s_2 \rrbracket, \llbracket e'_2 \rrbracket : T_3 )</td>
<td>( \ell ) fresh</td>
<td>( T_1 \sim T_3 )</td>
</tr>
<tr>
<td>( \Gamma \vdash \llbracket e_1 \ e_2 \rrbracket \sim \llbracket s_1 \ s_2 \rrbracket \ return \ e'_1 (e'_2 : (T_3 \Rightarrow (T_1)^\ell)); ] : T_2 )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \Gamma \vdash \llbracket e_1 \rrbracket \sim \llbracket s_1 \rrbracket, \llbracket e'_1 \rrbracket : \star )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \Gamma \vdash \llbracket e_2 \rrbracket \sim \llbracket s_2 \rrbracket, \llbracket e'_2 \rrbracket : T_1 )</td>
<td>( \ell ) fresh</td>
<td></td>
</tr>
<tr>
<td>( \Gamma \vdash \llbracket e_1 \ e_2 \rrbracket \sim \llbracket s_1 \ s_2 \rrbracket \ return \ (e'_1 : (\star \Rightarrow (T_2 \Rightarrow (T_1)^\ell)) (e'_2)); ] : \star )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \Gamma \vdash \llbracket e \rrbracket \sim \llbracket s_1 \rrbracket \ return \ e'_1 ; ] : T_2 )</td>
<td>( \ell ) fresh</td>
<td></td>
</tr>
<tr>
<td>( \Gamma \vdash \llbracket e : T_1 \rrbracket \sim \llbracket s_1 \rrbracket \ return \ (e' : (T_2 \Rightarrow (T_1)^\ell)); ] : T_1 )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \Gamma \vdash \llbracket e : T_1 \rrbracket \sim \llbracket s_1 \rrbracket \ return \ e_1(e_2) ; ] : T_2 )</td>
<td>( \ell ) fresh</td>
<td></td>
</tr>
<tr>
<td>( \Gamma \vdash \llbracket e : T_1 \rrbracket \sim \llbracket s_1 \rrbracket \ return \ c_1(e_2) ; ] : T_2 )</td>
<td>( \ell ) fresh</td>
<td></td>
</tr>
<tr>
<td>( \Gamma \vdash \llbracket \ell : T_1 \rrbracket \sim \llbracket s_1 \rrbracket \ return \ e_1(e_2) ; ] : T_2 )</td>
<td>( \ell ) fresh</td>
<td></td>
</tr>
</tbody>
</table>

Fig. 18. Coercion insertion and conversion to ANF for guarded objects, part 2.
Fig. 19. Value and store typing judgment for guarded objects.

\[
\begin{align*}
\Sigma &\vdash v : T \\
\Sigma &\vdash n : \text{int} \quad \Sigma &\vdash \text{true} : \text{bool} \quad \Sigma &\vdash \text{false} : \text{bool} \\
\forall l \in \text{dom}(A_1). \Sigma(A_1(l)) &= \Delta_1(l) \\
\forall l \in \text{dom}(A_2). \Sigma(A_2(l)) &= [\Delta_1; \Delta_2] \rightarrow \Delta_2(l) \\
\Sigma &\vdash [A_1; A_2 : [\Delta_1; \Delta_2] \\
\Gamma &\vdash \rho \quad \Gamma(x := T_1) &\vdash \pi : T_2 \\
\Sigma &\vdash (\lambda x. \pi. \rho) : T_1 \rightarrow T_2 \\
\Gamma &\vdash \rho \quad \Gamma(x := T_2)(y := (T_1 \rightarrow T_2, T_2 \rightarrow T_2)) &\vdash \pi : T_4 \\
\Sigma &\vdash (\lambda x. \pi. \rho, \nu) : T_3 \rightarrow T_4 \\
\Sigma &\vdash (\lambda x. \pi. \rho, (\nu; (T_1 \rightarrow T_2))] : * \\
\Sigma &\vdash \nu : T_1 \quad \Sigma &\vdash \nu; \Delta_2 : T_2 \\
\Sigma &\vdash \mu \\
\forall a \in \text{dom}(\Sigma). \Sigma &\vdash \mu(a) : \Sigma(a) \\
\end{align*}
\]

Fig. 20. The type system of the intermediate language for monotonic objects.
Fig. 21. Modifications to coercion insertion for monotonic objects.
\[ \vdash \text{static}(T) \]
\[ \vdash \text{static}(T_1) \quad \vdash \text{static}(T_2) \]
\[ \forall l \in \text{dom}(\Delta_1). \vdash \text{static}(\Delta_1(l)) \]
\[ \forall l \in \text{dom}(\Delta_2). \vdash \text{static}(\Delta_2(l)) \]
\[ \vdash \text{static}(T_1 \rightarrow T_2) \]
\[ \vdash \text{static}(\varnothing; \varnothing) \]

**Fig. 22.** Fully-static types

\[ \text{toplabel}(L) = p \]
\[ \text{toplabel}(B^p) = p \]
\[ \text{toplabel}([A_1; A_2]^p) = p \]
\[ \text{toplabel}(L_1 \rightarrow^p L_2) = p \]

\[ [L] = T \]
\[ \llbracket \ast \rrbracket = \ast \]
\[ \llbracket B^p \rrbracket = B \]
\[ \llbracket [A_1; A_2]^p \rrbracket = [A_1]; [A_2] \]
\[ \llbracket L_1 \rightarrow^p L_2 \rrbracket = [L_1] \rightarrow [L_2] \]
\[ [A](l) = [A(l)] \]

\[ [T]^p = L \]
\[ \llbracket B^p \rrbracket = B^p \]
\[ \llbracket \ast \rrbracket^p = \ast \]
\[ \llbracket T_1 \rightarrow T_2 \rrbracket^p = [T_1]^p \rightarrow [T_2]^p \]
\[ \llbracket \Delta_1; \Delta_2 \rrbracket^p = [[\Delta_1]^p; [\Delta_2]^p]^p \]
\[ \llbracket \Delta \rrbracket^p(l) = [\Delta(l)]^p \]

**Fig. 23.** Some operations on labeled types.
\( \Sigma \vdash v : T \)

\[\begin{array}{c}
\Sigma \vdash n : \text{int} & \Sigma \vdash \text{true} : \text{bool} & \Sigma \vdash \text{false} : \text{bool} \\
\forall l \in \text{dom}(A_1), \Sigma(A_1(l)) = \Delta_1(l) & \forall l \in \text{dom}(A_2), \Sigma(A_2(l)) = [\Delta_1; \Delta_2] \rightarrow \Delta_2(l) & \\
\Sigma \vdash [A_1; A_2] : [\Delta_1; \Delta_2] \\
\Gamma \vdash \rho \quad \Gamma(x := T_1) \vdash \pi : T_2 & \\
\Sigma \vdash (\lambda x. \pi, \rho, \epsilon) : T_1 \rightarrow T_2 & \\
\Gamma \vdash \rho \quad \Gamma(x := T_3)(y := (T_1 \rightarrow T_2, T_3 \rightarrow T_4)) \vdash \pi : T_4 & \\
\vdash \tau : T_1 \rightarrow T_2 \Rightarrow T_3 \rightarrow T_4 & \\
\Sigma \vdash (\lambda x. \pi, \rho, \tau) : T_3 \rightarrow T_4 \\
\Sigma \vdash (\lambda x. \pi, \rho, (\tau; (T_1 \rightarrow T_2(!)))) : * & \\
\Sigma \vdash \nu : I \quad \vdash I ! : I \Rightarrow * & \\
\Sigma \vdash \nu; I ! : * \\
\Sigma \vdash \mu \\
\forall a \in \text{dom}(\Sigma), \Sigma \vdash \mu(a) : [\mu(a)_1] \quad [\mu(a)_2] \leq_n \Sigma(a) & \\
\Sigma \vdash \mu
\end{array}\]

**Fig. 24.** Value and store typing judgment for monotonic objects.