Threesome, with and without blame

Citation for published version:

Digital Object Identifier (DOI):
10.1145/1706299.1706342

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Publisher's PDF, also known as Version of record

Published In:
Proceedings of the 37th annual ACM SIGPLAN-SIGACT symposium on Principles of Programming Languages (POPL '10)

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.
Abstract
How to integrate static and dynamic types? Recent work focuses on casts to mediate between the two. However, adding casts may degrade tail calls into a non-tail calls, increasing space consumption from constant to linear in the depth of calls.

We present a new solution to this old problem, based on the notion of a threesome. A cast is specified by a source and a target type—a twosome. Any twosome factors into a downcast from the source to an intermediate type, followed by an upcast from the intermediate to the target—a threesome. Any chain of threesomes collapses to a single threesome, calculated by taking the greatest lower bound of the intermediate types. We augment this solution with blame labels to map any failure of a threesome back to the offending twosome in the source program.

Herman, Tomb, and Flanagan (2007) solve the space problem by representing casts with the coercion calculus of Henglein (1994). While they provide a theoretical limit on the space over- head, there remains the practical question of how best to implement coercion reduction. The threesomes presented in this paper provide a streamlined data structure and algorithm for representing and normalizing coercions. Furthermore, threesomes provide a typed-based explanation of coercion reduction.

Categories and Subject Descriptors D.3.3 [Language Constructs and Features]: Procedures, functions, and subroutines
General Terms Languages, Theory
Keywords casts, coercions, blame tracking, lambda-calculus

1. Introduction
The old question of how to mix static and dynamic typing is attracting renewed interest. On one side, Hejlsberg (2008) brings type dynamic to C# 4.0, and on the other side, Tobin-Hochstadt and Felleisen (2008) integrate static types into Scheme and Wall (2009) adds optional static types to Perl 6. In these mixed settings, programmers and compilers should still be able to trust the results of the static type checker, so run-time checks are needed to safeguard the invariants established by the static type system. Recent work mediates between static and dynamic regions using casts.

Building on the higher-order contracts of Findler and Felleisen (2002), Wadler and Findler (2009) design the blame calculus to serve as an intermediate language that integrates static and dynamic typing. The blame calculus earns its name by tracking blame: it maps run-time type errors back to their origin in the source program. The Blame Theorem asserts that statically typed regions of a program can never be blamed for run-time type errors.

However, there is concern that the casts used in the blame calculus impose too much run-time overhead. Findler and Felleisen (2002) observed that contracts may degrade a tail call into a non-tail call and Herman et al. (2007) noted that the same is true for casts. This concern prompted the ECMAScript 4.0 committee (Hansen 2007) and the designers of Thorn (Wrigstad et al. 2009) to consider compromises such as like types that do not require casts.

Herman et al. (2007) use the coercion calculus of Henglein (1992, 1994) to represent and compress sequences of casts. Any coercion normalizes to a coercion of bounded size, thereby limiting the run-time space overhead to a constant factor. Siek et al. (2009) augment the coercion calculus with blame tracking to obtain a space-efficient implementation of the blame calculus.

In this paper we present a new solution to the space problem, based on the notion of a threesome. Traditionally, a cast is specified by a source and a target type—a twosome. We show that any twosome factors into a downcast from the source to an intermediate type, followed by an upcast from the intermediate to the target—a threesome. We also show that any chain of threesomes collapses to a single threesome, calculated by taking the greatest lower bound of the intermediate types. We then augment this solution with blame labels so as to map any failure of a threesome back to the offending twosome in the source program.

Threesomes are designed to correspond to twosomes and twosomes are designed to correspond to Henglein’s coercions. So it is not surprising that threesomes correspond to Henglein’s coercions. Nonetheless, it is a pleasant validation of our design that threesomes turn out to be exactly isomorphic to Henglein’s coercions in normal form. Coercion normalization is an iterative process, whereas composition of threesomes is a direct recursive definition. Thus, we believe that the alternative view offered by threesomes may make possible a more efficient implementation than one based directly on the coercion calculus.

The rest of the paper begins with a review of the blame calculus (Section 2). Then, to factor the presentation of the threesome calculus, we present a simplified version that captures the main intuitions and detects cast failures appropriately, but does not track blame (Section 3). We prove that the simplified version is correct and space efficient. Section 4 presents the complete threesome calculus with support for blame tracking and proves that it is correct (equivalent to the blame calculus). Section 5 shows that the threesome calculus is isomorphic to a coercion-based calculus of Siek et al. (2009). Some of the proofs are in-line and the rest are in the Appendix. We explain the relationship between our results and prior work in Section 6.
2. Twosomes

The definition of the blame calculus (minus subset types) is shown in Figure 1. This blame calculus is the simply-typed lambda calculus extended with the dynamic type, written \(\text{Int} \rightarrow \text{Bool} \rightarrow \text{Bool} \). We sometimes elide the blame label \(l\) on a cast when the label is not relevant. The meta-variable \(x\) ranges over variables, \(k\) over constants, and \(B\) over base types (such as \(\text{Int}\) and \(\text{Bool}\)). We give function application higher precedence than casts. The meta-variables \(l, m\) and \(n\) range over blame labels. In an implementation, blame labels would not be visible to the programmer, but would be inserted automatically by the parser and would provide access to information such as the location of the cast in the source program.

The dynamic semantics of the cast is straightforward in the case of first-order values such as integers: the run-time check either succeeds and the cast acts like the identity function, or the check fails and the downcast is blamed.

\[
\begin{align*}
\langle \text{Int} \rightarrow \text{Int} \rangle & \rightarrow \langle \text{Int} \rightarrow \text{Int} \rangle \\
\langle \text{Bool} \rightarrow \text{Int} \rangle & \rightarrow \langle \text{Bool} \rightarrow \text{Int} \rangle \\
\langle \text{Int} \rightarrow \text{Int} \rangle & \rightarrow \text{blame } m
\end{align*}
\]

Higher-Order Casts

The semantics of casts is more subtle in the case of higher-order casts such as functions. The complication is that one cannot immediately check whether a function respects the target type of the cast. In the example below, when the function \(f\) of type \(\text{Int} \rightarrow *\) is cast to \(\text{Int} \rightarrow \text{Int}\), there is no way to immediately tell if the function will return an integer every time it is called.

\[
\begin{align*}
\text{let } f &= \langle \lambda x : \text{Int}. \text{ if } 0 \leq x \text{ then } (* \rightarrow \text{Int})/2 \\
\text{else } (* \rightarrow \text{Bool})/\text{true} \rangle \text{ in } \\
\text{let } g &= \langle \text{Int} \rightarrow \text{Int} \rightarrow \text{Int} \rightarrow \text{Int} \rangle f \text{ in } \ldots
\end{align*}
\]

So long as \(g\) is only called with non-negative numbers, the behavior of \(f\) respects the type. If \(g\) is ever called with a negative number, the return value of \(f\) will induce a cast error.

The standard solution defers the check until the function is applied to an argument. When a function passes through a cast, the cast is not reduced but remains as a wrapper around the function. When the cast-wrapped function is applied to a value, then the cast is distributed to the argument and result as specified by the following reduction rule. Note that the direction of the cast on the argument is flipped, as usual. (Also the blame label of the cast on the argument is negated; we discuss this further below.)

\[
\begin{align*}
\langle (S' \rightarrow T' \leftarrow S \rightarrow T) \rangle & \rightarrow \langle (T' \rightarrow T) \rangle v ((S' \rightarrow S)' w)
\end{align*}
\]

Blame Tracking

Because a higher-order cast is not checked immediately, it might fail at a location far removed from where it was originally applied. Continuing the above example, the cast-wrapped function bound to \(g\) may be applied at some point much later in the program.

\[
\begin{align*}
\text{let } g &= \langle \text{Int} \rightarrow \text{Int} \rightarrow \text{Int} \rightarrow * \rangle f \text{ in } \\
\ldots \text{ g } \langle -1 \rangle \ldots
\end{align*}
\]

Blame tracking helps to diagnose such failures by mapping cast failures back to their origin in the source program. The above example reduces to \(\text{blame } n\), indicating that the cast surrounding \(f\) caused the failure. Figure 1 shows the reduction rules we use in this paper. The formulation here differs in minor ways from the rules of Wadler and Findler (2009) that will prove technically convenient. The most significant changes are that we allow casts between any two types, even if they are not compatible; and we introduce an empty type \(\perp\), such that no value has type \(\perp\) and \(\perp\) is incompatible with every type.

Blame labels come equipped with a negation operator that is an involution. That is, if \(m\) is a blame label then \(\overline{m}\) is its negation and \(\overline{\overline{m}} = m\). If a program halts with blame \(m\), the term contained inside the cast labeled \(m\) failed to produce a value of the appropriate type. If a program halts with blame \(\overline{m}\), the context surrounding the cast labeled \(m\) misused the cast value, that is, applied it to a value of an inappropriate type.

The blame calculus checks higher-order casts lazily, reporting blame for an incompatible cast on a function only when the function is applied. For example,

\[
\text{let } g = \langle \text{Int} \rightarrow \text{Int} \rightarrow \text{Bool} \rightarrow \text{Bool} \rangle f \text{ in } \ldots
\]

will fail only if \(g\) is applied. This is achieved by testing for shallow incompatibility between types. We write \(S \neq T\) to indicate shallow incompatibility. Distinct base types are shallowly incompatible, a function is shallowly incompatible with any base type, and the type \(\perp\) is shallowly incompatible with any type.

In the definition of values, we add a side condition on values of the form \((S' \rightarrow T' \leftarrow S \rightarrow T)\). We require that not all \(S, T, S', T'\) be \(\perp\) because otherwise rule (3) would apply.

In this paper we restrict our attention to lazy checking. Siek et al. (2009) discuss other design points, such as eager checking (where any incompatibility is reported as soon as possible). An initial assessment indicates that it would be straightforward to apply the techniques in this paper to the other designs.

Space Efficiency

Herman et al. (2007) observe two circumstances where the wrappers used for higher-order casts can lead to unbounded space consumption. First, some programs repeatedly apply casts to the same function, resulting in a build-up of wrappers. In the following example, a wrapper is added each time the function bound to \(k\) is passed between even and odd, causing a space leak proportional to \(n\).

\[
\begin{align*}
\text{let } \text{rec } \text{even}(n : \text{Int}, k : \rightarrow \text{Bool}) \text{ : } \text{Bool} &= \text{if } (n = 0) \text{ then } k(\text{false}) \text{ else } \text{odd}(n - 1, \text{Bool} \leftarrow \text{Bool} \leftarrow \text{Bool} \leftarrow k) \\
\text{and } \text{odd}(n : \text{Int}, k : \text{Bool} \rightarrow \text{Bool} : \text{Bool} &= \text{if } (n = 0) \text{ then } k(\text{true}) \text{ else } \text{even}(n - 1, \text{false} \rightarrow \text{Bool} \leftarrow \text{Bool} \leftarrow k)
\end{align*}
\]

Second, some casts break tail recursion. Consider the following example in which the return type of even is \(\ast\) and odd is \(\text{Bool}\).

\[
\begin{align*}
\text{let } \text{rec } \text{even}(n : \text{Int}) : \ast &= \text{if } (n = 0) \text{ then } (\ast \leftarrow \text{Bool})/\text{true} \text{ else } (\ast \leftarrow \text{Bool})/\text{false} \\
\text{and } \text{odd}(n : \text{Int}) : \text{Bool} &= \text{if } (n = 0) \text{ then } \text{false} \text{ else } (\text{Bool} \leftarrow \ast)/\text{even}(n - 1)
\end{align*}
\]

Assuming tail call optimization, cast-free versions of the even and odd functions require only constant space. However, with the presence of casts, the calls to even and odd are not tail calls, so the run-time stack grows with each call and space consumption is proportional to \(n\). The following reduction sequence for a call to even shows the unbounded growth.

\[
\begin{align*}
\text{even}(n) & \rightarrow (\ast \leftarrow \text{Bool})/\text{odd}(n - 1) \\
& \rightarrow (\ast \leftarrow \text{Bool})/\text{false} \\
& \rightarrow (\ast \leftarrow \text{Bool})/\ast \\
& \rightarrow (\ast \leftarrow \text{Bool})/\text{even}(n - 3) \\
& \rightarrow \ldots
\end{align*}
\]

Herman et al. (2007) recover space efficiency in a cast calculus without blame by 1) using the coercion calculus (Henglein 1994) to compactly represent sequences of casts, and 2) normalizing sequences of coercions that appear in tail-position before making function calls. Siek et al. (2009) extend this work by integrating blame tracking into the coercion calculus, thereby achieving a
3. Threesomes Without Blame

The goal of the threesome calculus is to achieve space efficiency while maintaining the high-level nature of the blame calculus, that is, expressing casts with types. The key to space efficiency is to compress sequences of casts while maintaining the same behavior. There are two aspects to the behavior of a cast: 1) detecting cast failures and 2) allocating blame to the appropriate cast in the source program. In this section we describe a simplified version of the threesome calculus that focuses on detecting cast failures. In relating the simplified threesome calculus to the blame calculus, we ignore all blame labels in the blame calculus. In Section 4 we present the complete threesome calculus with blame tracking.

When discussing a sequence of casts, we abbreviate
\[ \langle T_n \leftarrow T_{n-1} \rangle \cdots \langle T_3 \leftarrow T_2 \rangle \langle T_2 \leftarrow T_1 \rangle \]
as follows to avoid repeating types.
\[ \langle T_n \leftarrow T_{n-1} \cdots T_3 \leftarrow T_2 \leftarrow T_1 \rangle \]

Towards understanding how to compress casts, consider the following sequence:
\[ \langle * \rightarrow * \leftarrow \text{Bool} \rightarrow * \leftarrow \text{Int} \leftarrow * \rightarrow * \rangle \]

This sequence, when applied to a function, forces the function to accept an argument of type \text{Bool} and to return a result of type \text{Int}; any other argument or result induces an error. Thus, the above sequence of casts is equivalent to just two casts where the intermediate type is \text{Bool} \rightarrow \text{Int}.
\[ \langle * \rightarrow * \leftarrow \text{Bool} \rightarrow \text{Int} \leftarrow * \rightarrow * \rangle \]

The type \text{Bool} \rightarrow \text{Int} represents a stronger cast, one that is more likely to fail, than either of the two intermediate types in the original sequence. This notion of stronger is captured by the naive subtyping relation, written \text{<}., of Wadler and Findler (2007) (defined in Figure 2); similar relations include the \text{\leq} ordering on coercions of Henglein (1994) and the \text{\leq} ordering on retracts of Scott (1976). Our idea is to compress a sequence of casts into just two casts where the intermediate type is the greatest lower bound of the types in the original sequence.

Naive subtyping is covariant in the domain of function types instead of contravariant like ordinary subtyping. It is interesting to compare taking the greatest lower bound with respect to naive subtyping versus ordinary subtyping. In the above example, with naive, covariant subtyping we have
\[
\begin{align*}
\text{Bool} \rightarrow \text{Int} &<; \text{Bool} \rightarrow \text{Int} \\
\text{Bool} &<; \text{Bool} \rightarrow \text{Int} \\
\end{align*}
\]
and so the greatest lower bound of the original casts with regard to \text{<} is \text{Bool} \rightarrow \text{Int}, which has the desired effect. In contrast, with ordinary, contravariant subtyping (written \text{\langle} < \text{\rangle}) we have
\[ \langle * \rightarrow * \leftarrow \text{Bool} \rightarrow * \rangle \]
So the greatest lower bound of the original casts with regard to \text{\langle} is \text{\langle} * \rightarrow \text{Int} \text{\rangle}. Using this as the intermediate type gives a different collapsed cast
\[ \langle * \rightarrow * \leftarrow * \rightarrow \text{Int} \leftarrow * \rightarrow * \rangle \]
But this cast is too lenient; it correctly requires the result to be \text{Int} but does not require the argument to be \text{Bool}.

We write \text{S} \& \text{T} for the greatest lower bound of \text{S} and \text{T} with respect to \text{<}; we also sometimes call this the meet of \text{S} and \text{T}. In general, an arbitrary sequence of casts can collapse to a contextually equivalent pair of casts where the intermediate type is the meet of all the types in the sequence, so
\[ \langle T_n \leftarrow T_{n-1} \cdots \leftarrow T_2 \leftarrow T_1 \rangle \]
is equivalent to
\[ \langle T_n \leftarrow T_{n-1} \& \cdots \& T_2 \& T_1 \rangle \]
We introduce a special notation for casts of this kind. For any three types \text{R}, \text{S}, \text{T} with \text{R} \langle; \text{S} and \text{R} \langle; \text{T}, and any term \text{t} of type \text{S}, we write
\[ \langle T \leftarrow \text{R} \rangle \langle \text{R} \leftarrow \text{S} \rangle \text{t} \]
and call it a threesome. It is equivalent to the pair of casts
\[ \langle T \leftarrow \text{R} \rangle \langle \text{R} \leftarrow \text{S} \rangle \text{t} \]

The syntax of the threesome calculus without blame is given in Figure 2. Analogously to the side condition on values for twosomes,
we require that in a value of the form \((T \rightarrow T' R \sqsubseteq R' S \rightarrow S')u\),
not all of \(T, T', R, R', S\) and \(S'\) can be \(*\).

Greatest lower bounds can be computed by the algorithm for \(S \& T\) defined in Figure 2. The algorithm is straightforward: the
meet of identical base types is that base type, of two function types
is a function from the meet of the domains to the meet of the
ranges, of any type with * is the other type, and of any shallowly
incompatible types is \(\perp\). Note that the greatest lower bound always
exists thanks to the inclusion of the empty type \(\perp\). Since \(S \& T\) is
symmetric, the reader may wonder why we write \(T \& S\) in the clause
for function types; this is foreshadowing modifications required in
the next section for tracking blame.

Our first result is to confirm that the algorithm in Figure 2
computes greatest lower bounds.

**Proposition 1** (Meet algorithm returns the greatest lower bound),
1. \(S \& T \sqsubseteq n\ S\) and \(S \& T \sqsubseteq n\ T\).
2. If \(R \sqsubseteq n\ S\) and \(R \sqsubseteq n\ T\), then \(R \sqsubseteq n\ S \& T\).

The operational semantics of the threesome calculus is given in
Figure 2. Most of the reduction rules are a straightforward adapta-
tion from twosomes to threesomes. For example, rule (13) is equiv-
alent to two applications of rule (3) from the blame calculus. The
difference is the addition of rule (16), which is responsible for
compressing a pair of threesomes into a single threesome by taking
the meet of the two intermediate types. The source and target types
of a threesome do not play a role in the reduction rules and could
be erased but their presence streamlines the meta-theory by giving
us unicity of types.

To make sure that sequences of casts do not accumulate in tail
position, we change evaluation contexts to recognize sequences of
casts outside-in, repeatedly compressing the two outermost
position, we change evaluation contexts to recognize sequences of
values.

The context \(E\) includes both the
appropriate location to apply a cast-reducing rule. The context
includes both the \(F\) contexts and contexts containing sequences of
casts with length at most one.

This formulation of evaluation contexts differs from the con-
texts used in Herman et al. (2007). Unique decomposition does not
hold for their contexts, for example, in a sequence of three casts,
either the outer two or the inner two can be merged. However,
because the coercion calculus is confluent, the lack of unique decom-
position does not pose a serious problem. Nevertheless, we prefer
to use evaluation contexts that ensure a unique decomposition.

**Proposition 2** (Unique Decomposition). For a well-typed closed \(t\),
either \(t\) is a value or there is a unique decomposition into a redex
\(t'\) and an evaluation context \(E\) such that \(t = E[t']\).

The values of the threesome calculus differ in an important way
from the blame calculus, which reflects the improved space effi-
ciency. In the blame calculus, a value of type \(T \rightarrow T'\) may contain
an arbitrary number of outermost casts. In the threesome calculus,
a value of type \(T \rightarrow T'\) may contain at most one outermost cast.

**Lemma 1** (Canonical Forms).
1. If \(\emptyset \vdash v : B\), then \(v\) is a constant.
2. If \(\emptyset \vdash v : T \rightarrow T'\), then \(v\) has one of the following forms:
\(\lambda x : S.t\), or \((T \rightarrow T' R \sqsubseteq R' S \rightarrow S')u\).
3. If \(\emptyset \vdash v : *\), then \(v\) has the form \((* \sqsubseteq S)u\).
4. No value has type \(\perp\).

**Proof.** The proofs are by case analysis on \(v\) and inversion on the
typing rules.

**Syntax**

- **terms** \(s, t \::= k \mid x \mid \lambda x : S.t \mid s t \mid (T \sqsubseteq R S)u\)
- **uncoerced val** \(u \::= k \mid \lambda x : S.t\)
- **values** \(v, w \::= u \mid (* \sqsubseteq S)u \mid (T \rightarrow T' R \sqsubseteq R' S \rightarrow S')u\)
- **contractums** \(r \::= t \mid \text{blame}\)
- **cast-free contexts** \(F \::= \square \mid E[F] \mid E[v] \square\)
- **eval contexts** \(E \::= F \mid (F \sqsubseteq T \sqsubseteq S)\square\)

**Naive subtyping**

\[B \sqsubseteq n\ B \sqsubseteq n\ S \sqsubseteq n\ T \sqsubseteq n\ S' \sqsubseteq n\ T'\]

**Additional typing rules**

\[\Gamma \vdash s : S \quad R \sqsubseteq n\ S \quad R \sqsubseteq n\ T\]
\[\Gamma \vdash (T \sqsubseteq R S)u : T\]

**Meet algorithm** (computes the greatest lower bound)

\(S \& T\)

\[\emptyset \vdash s : S \quad \emptyset \vdash t : T\]
\[\emptyset \vdash (T \sqsubseteq R S)u : T\]

**Reductions**

\(\langle \lambda x : S.t \rangle v \rightarrow [x := v]t\)

\(k k' \rightarrow \delta(k, k')\)

\(\langle (T \rightarrow T' R \sqsubseteq R' S \rightarrow S')u \rangle w \rightarrow (T' \sqsubseteq R S)u \langle (S \sqsubseteq R T)w \rangle\)

if not \(T \rightarrow T' = R \rightarrow R' = S \rightarrow S' = \ast \rightarrow \ast\)

**Cast reductions**

\([G \leq \overrightarrow{C} G]u \rightarrow e u\)

\([\ast \sqsubseteq \ast]u \rightarrow e u\)

\([T \sqsubseteq S]u \rightarrow \text{blame}\)

\([T \sqsubseteq S'] \langle T' \sqsubseteq R S \rangle u \rightarrow e \langle T' \sqsubseteq R \sqsubseteq S \rangle s\]

**Single-step evaluation**

\(E[t] \rightarrow E[t']\)

\(F[e] \rightarrow F[t']\)

\(F[t] \rightarrow \text{blame}\)

**Figure 2.** Threesomes without blame

**3.1 Correspondence Between Twosomes and Threesomes**

We translate from the blame calculus to the threesome calculus by
mapping casts of the form \(\langle T \equiv S \rangle s\) to \(\langle T \sqsubseteq R \sqsubseteq S \rangle s\). The
definitions for compiling twosomes to threesomes, and decompil-
ing threesomes to twosomes, written \(\langle t \rangle\) and \(\langle t \rangle^{-1}\) respectively,
are given in Figure 3.

The proof that the threesome calculus without blame is equiv-
alent to the blame calculus (ignoring blame labels) hinges on two
facts. First, the cast \(\langle T \equiv S \rangle\) is equivalent to \(\langle T \equiv T \& S \equiv S \rangle\).
This is necessary to justify the compilation from twosomes to thres-
somes. Second, \(\langle T \equiv R \equiv S' \equiv R \equiv S \rangle\) is equivalent to
Compilation from twosomes to threesome
\[
\langle \langle t \rangle \rangle = t
\]
\[
\langle x \rangle = x \hspace{1cm} \langle k \rangle = k
\]
\[
\langle \lambda x : S \ t \rangle = \lambda x : S. \langle \langle t \rangle \rangle
\]
\[
\langle \langle T \leftarrow S \rangle \rangle = \langle T \leftarrow S \rangle \langle \langle S \rangle \rangle
\]

Decomposition from threesome to twosomes
\[
\langle \langle t \rangle \rangle^{-1} = t
\]
\[
\langle \langle x \rangle \rangle^{-1} = x \hspace{1cm} \langle \langle k \rangle \rangle^{-1} = k
\]
\[
\langle \lambda x : S \ t \rangle^{-1} = \lambda x : S. \langle \langle t \rangle \rangle^{-1}
\]
\[
\langle \langle T \leftarrow R \rangle \rangle^{-1} = \langle T \leftarrow (R \leftarrow \langle \langle S \rangle \rangle \langle \langle S \rangle \rangle^{-1}
\]

Figure 3. From twosomes to threesomes and back again.

\[ (T \leftarrow R & R \leftarrow S) \text{ provided } R' <_{<} T, R' <_{<} S', R <_{<} S', \text{ and } R <_{<} S. \text{ This fact is necessary to justify the threesome reduction rule (16), which compresses two threesomes. Both of these facts are corollaries of the following fundamental lemma. In a sequence } (T \leftarrow R \leftarrow S), \text{ it is safe to bypass } R \text{ if going from } S \text{ to } T \text{ to } R \text{ is an upcast.} \]

Towards formalizing this in terms of contextual equivalence, we define contexts and results as follows.

\[
\begin{align*}
\text{contexts } & \quad C := \emptyset \mid C \cup T \mid C \cup \lambda x : S. C \mid (T \leftarrow S)C \\
\text{results } & \quad f := v \mid \text{blame}
\end{align*}
\]

A program \( t \) is said to be convergent, written \( t \downarrow \), if \( \exists f, t \leadsto^* f \), where \( \leadsto^* \) is the reflexive, transitive closure of \( \leadsto \). These definitions for twosomes carry over easily to the threesome calculus.

**Definition 1.** A term \( t \) is contextually equivalent to another term \( t' \), written \( t =_{\text{ctx}} t' \), if for any context \( C \), \( C[t] \Downarrow \text{iff } C[t'] \Downarrow \).

**Lemma 2 (Fundamental Property of Casts).**

If \( T <_{<} S \), then \( (T \leftarrow R \leftarrow S) t =_{\text{ctx}} (T \leftarrow S) t \).

The proof of the fundamental property of casts is in the Appendix. With this property in hand we can prove the two key facts.

**Corollary 1.**

1. \( (T \leftarrow S) s =_{\text{ctx}} (T \leftarrow T & S \leftarrow S) s \) and
2. \( (T \leftarrow R' \leftarrow S' \leftarrow R \leftarrow S) s =_{\text{ctx}} (T \leftarrow R' & R \leftarrow R \leftarrow S) s \) provided \( R' <_{<} T, R' <_{<} S', R <_{<} S', \text{ and } R <_{<} S. \)

**Proof.**

1. Note that subtyping is reflexive and then apply the fundamental property of casts.
2. To prove the second part, we apply the fundamental property of casts several times as follows.

\[
\begin{align*}
(T \leftarrow R' \leftarrow S' \leftarrow R \leftarrow S) s =_{\text{ctx}} (T \leftarrow R' \leftarrow R \leftarrow S) s \\
=_{\text{ctx}} (T \leftarrow R' \leftarrow R & R \leftarrow R \leftarrow S) s \\
=_{\text{ctx}} (T \leftarrow R' & R \leftarrow R \leftarrow R \leftarrow S) s \\
=_{\text{ctx}} (T \leftarrow R' & R \leftarrow S) s
\end{align*}
\]

We need a few more facts before proving the correctness theorem.

**Lemma 3.** \( t =_{\text{ctx}} \langle \langle \langle t \rangle \rangle \rangle^{-1} \).

**Proof.** The proof is by induction on \( t \). The case for casts relies on Corollary 1 (part 1).

**Lemma 4.**

1. If \( t =_{\text{ctx}} \langle \langle t_3 \rangle \rangle^{-1} \) and \( t_3 \leadsto^* t'_3 \), then \( t =_{\text{ctx}} \langle \langle t'_3 \rangle \rangle^{-1} \).
2. If \( t_3 =_{\text{ctx}} \langle \langle t \rangle \rangle \) and \( t \leadsto^* t' \), then \( t_3 =_{\text{ctx}} \langle \langle t' \rangle \rangle \).

**Proof.**

1. The proof is by induction on \( t_3 \leadsto^* t'_3 \) and by cases on \( \leadsto^* \). The case for rule (16) relies on Corollary 1 (part 2). The other cases rely on the fact \( \leadsto^* \) implies \( t =_{\text{ctx}} t' \).

2. The proof is by induction on \( t \leadsto^* t' \) and by cases on \( \leadsto^* \). The cases rely on Lemma 2 and the fact \( t_3 \leadsto^* t'_3 \) implies \( t_3 =_{\text{ctx}} t'_3 \).

Applying compilation or decomposition to results produces terms that converge.

**Lemma 5.** \( \langle \langle f \rangle \rangle \Downarrow \text{ and } \langle \langle f \rangle \rangle^{-1} \Downarrow \).

**Proof.** The proofs are by induction on \( f \text{ and } f_3 \).

We can now state and prove the correctness theorem.

**Theorem 1** (Correctness of the threesome calculus without blame). \( \langle \langle t \rangle \rangle \Downarrow \text{ if and only if } t \Downarrow \).

**Proof.** By Lemma 3 we have \( t =_{\text{ctx}} \langle \langle \langle t \rangle \rangle \rangle^{-1} \).

1. \( (\Rightarrow) \) We have an \( f_3 \) such that \( \langle \langle t \rangle \rangle \leadsto^* f_3 \). Then by Lemma 4 (part 1) we have \( t =_{\text{ctx}} \langle \langle f_3 \rangle \rangle^{-1} \). Then by Lemma 5, \( t \Downarrow \).

2. \( (\Leftarrow) \) We have an \( f \) such that \( t \leadsto^* f \). Then by Lemma 4 (part 2) we have \( \langle \langle f \rangle \rangle =_{\text{ctx}} \langle \langle f \rangle \rangle \). Then by Lemma 5, \( \langle \langle f \rangle \rangle \Downarrow \).

**3.2 Space Efficiency**

The main task in bounding the size of casts during execution is to put a bound on the result of merging two casts. The approach taken by Herman et al. (2007) for the coercion calculus is to show that the height of a composed coercion is no greater than the height of the two coercions. Then, because normalized coercions are trees with limited branching, it follows that the size of the composed coercion is bounded by roughly \( 2^h \) where \( h \) is the height.

We obtain a tighter bound for the threesome calculus that takes into account that when two casts are composed, there is often considerable overlap between the two intermediate types, and therefore the resulting size of the new intermediate type is not much larger. (We take the size of a type to be the number of nodes in the type when considered as an abstract syntax tree.) A strawman for the bound is the size of the greatest lower bound of all the types that occur in the program. The problem with this strawman is that the greatest lower bound of two types can sometimes be smaller, thereby not providing an upper bound on size. For example, \( \text{Int} \) \& \( \ast \to \ast \) is \( \bot \). Instead we need to take the maximum of the structure of the two types. To accomplish this we map types to their shadow, written \( [T] \), and then compute the greatest lower bound. We define the shadow of a type as follows.

\[
\begin{align*}
[B] &= \ast \\
[S \to T] &= [S] \to [T] \\
[\ast] &= \ast \\
[\bot] &= \ast
\end{align*}
\]

With the previous example, we have \( [\text{Int}] \) \& \( \ast \to \ast \) is \( \ast \to \ast \).

**Proposition 3** (Properties of shadows).

1. \( \text{size}(T) = \text{size}([T]) \).
2. If \( R <_{<} [S] \) and \( R <_{<} [T] \) then \( R <_{<} [S \land T] \).
3. If \( [S] <_{<} [T] \), then \( \text{size}([T]) \leq \text{size}([S]) \).
We prove that the sizes of types in the program during reduction are bounded above by the greatest lower bound of the shadows of the types in the original program. The main lemma below shows that the greatest lower bound remains a lower bound during reduction. We can then apply the above property to show that the size of the greatest lower bound is an upper bound on the size of any type in the program. Towards formally stating these properties, we give the following definitions.

\[ T \in t \equiv T \text{ syntactically occurs in term } t \]
\[ \{ T \} \equiv | T | \mid T \in t \]
\[ S \ll T \equiv \forall T \in T. S \ll T \]
\[ \& (T_1, \ldots, T_n) \equiv T_1 \land \cdots \land T_n \]

**Lemma 6** (Preservation of lower bounds).

If \( T \ll \{ t \} \), and \( t \rightarrow t' \), then \( T \ll \{ t' \} \).

**Lemma 7** (Preservation of compilation).

If \( T \ll \{ t \} \), then \( T \ll \{ t' \} \).

**Theorem 2** (Bound on size of types and therefore casts).

If \( \{ t \} \rightarrow^* t' \), then for any \( T \in t' \), \( \text{size}(T) \leq \text{size}(\& \{ t \}) \).

Let \( | t | \) be the term \( t \) with all the casts erased. The size of a threesome program during execution does not differ by more than a constant factor to compared to itself with all the casts erased.

**Theorem 3** (Space efficiency).

For any program \( t \), if \( t \rightarrow^* t' \), then \( \text{size}(t') \leq \text{size}(\& t) \cdot \text{size}(t') \).

**Proof.** The proof is essentially the same as in Herman et al. (2007), except we use Theorem 2 for the bound on the size of types. \( \Box \)

## 4. Threesomes with Blame

In the previous section we showed that a simplified threesome calculus implements the blame calculus ignoring blame labels. We now turn our attention to adding correct blame allocation to the threesome calculus. Consider what would happen if we were to naively add blame labels to threesome casts, say, writing the blame label next to the intermediate type. When merging two casts, we would need to choose between label \( m \) and \( l \).

\[
\lambda f : \star \rightarrow \star. (\star \rightarrow \text{Bool} \rightarrow \star) \rightarrow (\star \rightarrow \text{Bool} \rightarrow \star) f
\]

\[
\lambda x : \star. (\star \rightarrow \text{Int}) | (\star \rightarrow \text{Bool}) \rightarrow \text{true} \rightarrow \text{blame } m
\]

Having just one blame label per cast is not enough.

The solution we propose is to incorporate blame labels into the intermediate type of a threesome. The above function \( g \) is then represented in the threesome calculus as follows.

\[
g = \lambda f : \star \rightarrow \star. (\star \rightarrow \text{Bool} \rightarrow \text{Bool} \rightarrow \star \rightarrow \star) f
\]

The label on the codomain of the intermediate type is \( m \) because cast \( m \) is the first (from left to right) to project from \( \ast \) to \( \text{Bool} \) in the codomain. The label on the domain \( l \) is because cast \( l \) is the first (from left to right) to project from \( \ast \) to \( \text{Bool} \). The function type itself is given the empty label \( e \) because in this sequence of casts, the function type cannot induce blame.

The definition of the threesome calculus with blame is given in Figure 4. The erasure of a labeled type \( P \) to a type is written \( \text{size}(P) \).
$G$ is the ground type that is shallowly compatible with $|P|$, and $p$ is the topmost blame label in $P$.

$$\text{gnd}(B^p) = B^p \quad \text{gnd}(P \to^p Q) = (\to^p)$$

In patterns, we write $P_{\geq p}$ to indicate that $P$ is a labeled type with $\text{gnd}(P) = G^p$.

The composition of labeled types is defined in Figure 4. In general, the label on the right-hand type takes precedence over the left-hand type. This is because the right-hand type induces a cast error before the left-hand side. The composition of two function types is a function type whose blame label is taken from the right-hand function type, whose range is the composition of the ranges of the two function types and whose domain is the reverse composition of the domains. This reversal mimics the contravariant behavior of function casts in the blame calculus; see rule (8).

Our treatment of the labeled bottom type $\bot_{\geq p}$ deserves some explanation. We initially tried to label bottom types with a single label, as in $\bot^n$. However, that approach fails to capture the correct blame tracking behavior. Consider the following examples.

\[
\begin{align*}
\text{(Int } \downarrow \epsilon & \equiv \text{ Bool } \downarrow \epsilon \equiv \text{ Int}) \quad \text{blame } n \\
\text{(Int } \downarrow \epsilon & \equiv \text{ Bool } \downarrow \epsilon \equiv \text{ Bool}) \quad \text{true } \quad \text{blame } l
\end{align*}
\]

Recall that in the threesome calculus, casts are merged outside-in. The two outermost casts would be merged into cast with middle type $\bot^n$. For the next merge, we could choose to produce either $\bot^n$ or $\bot^m$. However, either choice would be wrong for one of the above examples. Our solution is to label bottom types with not only a label, but also with a labeled ground type. So in this case, the second merge results in $\bot_{\leq \text{bool}}^n$.

One might wonder why the bottom type only needs to remember two labels and not more. A closer inspection of the composition rules dealing with bottom reveals why this is the case. When composing $\bot_{\leq \text{int}}^n$ with a labeled type $P_{\geq p}$ on the right, either $H$ is equal $G$, so $p$ overshadowed $q$ and the result is $\bot_{\leq \text{int}}^m$, or $H$ is not equal to $G$, and we have a new cast failure that needs to blame $q$. So we can forget the label $m$ and the result is $\bot_{\leq \text{bool}}^p$.

The following proposition expresses the relationship between composition and meet.

**Proposition 4.** $|Q \circ P| = |Q| \& |P|$

The main difference between the reduction rules for the threesome calculus, shown in Figure 4, and the rules for the simplified calculus is the use of the composition operator $\circ$ in place of the meet operator $\&$ in rule (23).

### 4.1 Correspondence Between Thowsomes and Threesomes

The compilation of the blame calculus to the threesome calculus, written $\llangle t \rrangle$, is given in Figure 5. The case for casts is a bit more complicated than for the simplified calculus, in that we must also define how to propagate labels into the intermediate type; function $\llangle T \overset{r}{\rightarrow} S \rrangle$ performs this duty and is defined in Figure 5. Its definition is straightforward, though two things are worth pointing out. The label is negated when going under the left-hand side of a function type and we put the empty label $\epsilon$ on types in situations where the cast could not produce blame, such as identity casts and injections. The following is the relationship between $\llangle T \overset{r}{\rightarrow} S \rrangle$ and meet.

**Proposition 5.** $\llangle T \overset{r}{\rightarrow} S \rrangle = T \& S.$

With the addition of blame labels, it is not as straightforward to establish the equivalence between the threesome calculus and the blame calculus because we can no longer merge casts in the blame calculus itself. However, we are able to construct a bisimulation relation, shown in Figure 6, linking reduction in the two systems. The bisimulation relates a sequence of thowsomes with a single threesome. To accomplish this, rule (25) peels off a threesome from the sequence and recursively relates a modified threesome with the rest of the sequence. The modification removes the contribution of the one threesome from the threesome’s intermediate type.

Rule (26) is necessary to relate states during the application of a cast-wrapped function to a value. On the blame calculus side, the function is wrapped in a sequence of casts and there is a sequence of reductions via rule (8). On the threesome side, there is only one cast and one reduction via rule (19). Rule (26) therefore relates the intermediate steps of the blame calculus back to the state of the thowsomes before the reduction via rule (19). Rule (27) is similar to rule (26) but handles the special case when $T_1 \rightarrow T_2 = |P| = S$.

**Lemma 8 (Bisimulation between the blame and threesome calculi).** If $s_2 \approx s_3$ and both $s_2$ and $s_3$ are well typed, then

1. if $s_2 \rightarrow r_2$, then $s_3 \rightarrow^* r_3$ and $r_2 \approx r_3$ for some $r_3$.
2. if $s_3 \rightarrow r_3$, then $s_2 \rightarrow^* r_2$ and $r_2 \approx r_3$ for some $r_2$. 
Towards proving the correctness of the threesome calculus, we show that compilation returns a threesome calculus program that is bisimilar to the source program.

**Lemma 9** (Compilation returns a bisimilar program.) \( t \equiv \llangle t \rrangle \)

Also, we show that the bisimulation is sound with respect to observable behavior.

**Lemma 10.** If \( t_3 \equiv t_4 \), then \( t_2 \downarrow \) if and only if \( t_3 \downarrow \).

The correctness of the threesome calculus is a straightforward consequence of these lemmas.

**Theorem 4** (Correctness of the threesome calculus). \( \llangle t \rrangle \downarrow \) if and only if \( t \downarrow \).

### 4.2 Space Efficiency

The addition of labels to the intermediate types of the threesomes only adds a constant factor increase in space, so the proof of space efficiency from Section 3.2 carries over to the full threesome calculus in a straightforward manner.

### 5. Relation to the Coercion Calculus

Henglein (1994) introduces a sub-language named the coercion calculus to express casts. Instead of casts of the form \((T \leq S)s\), Henglein uses casts of the form \((c)s\) where \(c\) is a term of the coercion calculus. The coercion calculus is not intended to be directly used by programmers, but instead casts of the form \((T \leq S)s\) are compiled into casts of the form \((c)s\). The coercion calculus precedes blame tracking, but Siek et al. (2009) augment the coercion calculus with blame, obtaining the calculus shown in Figure 7.

The coercion \(G!\) injects a value into \(*\) whereas the coercion \(G\) projects a value out of \(*\), blaming location \(l\) in the case of a type mismatch. The identity coercion \(\iota\) behaves like the identity function. The type annotation \(T\) on the identity coercion is always either a ground type or \(*\). A function coercion \(c \circ d\) applies coercion \(c\) to a function’s argument and \(d\) to its return value. Coercion composition \(d \circ c\) applies coercion \(c\) then coercion \(d\). We consider coercions equal up to associativity of composition. In addition to Henglein’s coercions, there is the Fail coercion of Herman et al. (2007), which compactly represents coercions that are destined to fail but have not yet been applied to a value.

The coercion reduction system we present here corresponds to Henglein’s notion of \(\psi\)-reduction: \(G! \circ G! \rightarrow \iota G\). Henglein also studied \(\psi\)-reduction: \(G! \circ G\) \(\rightarrow \iota G\). While \(\psi\)-reduction is useful when considering how best to compile dynamically typed languages (as in Henglein’s work), \(\psi\)-reduction is not suitable in our setting as it would allow some errors to go uncaught.

Rule (34) for composing failures on the left is subtle. Herman et al. (2007) instead use the reduction

\[
\text{Fail} \circ c \rightarrow \text{Fail}
\]

However, with the addition of blame tracking, that rule would violate the calculus non-deterministic. Siek et al. (2009) restrict \(c\) to injections.

\[
\text{Fail}^{T \leftarrow \iota} \circ G! \rightarrow \text{Fail}^{T \leftarrow \iota} \circ G!
\]

But that rule is useless because failure coercions never have \(*\) as a source type. To see why this is the case, first consider rule (29) which introduces failures; the source type is \(G\). Next, the only other way to obtain a failure with source type \(*\) would be to have a rule of the form

\[
\text{Fail}^{T \leftarrow \iota} \circ G! \rightarrow \text{Fail}^{T \leftarrow \iota} \circ G!
\]

but we certainly don’t want such a rule because that would introduce non-determinism. (The presence of the useless rule in the semantics of Siek et al. (2009) does not invalidate any of their results.)

In this paper, because we are using lazy cast checking, we can allow the coercion on the right to be a function coercion. With lazy checking, any errors in the domain or codomain of a cast appear after errors concerning the function type itself, even if the error concerning the function type appears later in a series of casts. For example, the following program allocates blame to \(l_4\) even though there is also a potential error at \(l_2\).

\[
\langle \text{Bool} \downarrow \rangle \text{Int} \rightarrow \text{Bool} \downarrow \langle \text{Int} \rangle \lambda x : \text{Int}. x \quad \text{blame } l_4
\]

We give an inductive characterization of the \(\psi\)-normal forms of the coercion calculus in Figure 7, writing \(nm \circ c\) for this inductive predicate.

**Proposition 6.** Suppose \(c : T \Leftarrow S, \text{nm } c\) if and only if \(\text{nm } c'\).

Figure 9 gives the definition of a coercion-based calculus with blame tracking similar to that of Siek et al. (2009). In this presentation we choose to keep coercions in normal form and perform coercion normalization in rule (39).

The correspondence between the threesome calculus and the coercion-based calculus is quite strong: threesome casts are isomorphic to well-typed coercions in normal form. Figure 8 defines the function and its inverse that witnesses this isomorphism.

**Proposition 7** \((\llangle \rrangle)\) produces a coercion in normal form.\(, \quad \text{If } P \llangle S, T \llangle P, s, \text{then } nm \llangle T \Leftarrow S \rrangle\).

**Lemma 11** (Bijection between threesomes and coercions). \(, \quad \text{If } |P| \llangle S, T \llangle P, \text{and } nm c, \text{then } \llangle T \Leftarrow S \rrangle = \llangle P \Leftarrow S \rrangle\).

The isomorphism is structure-preserving with respect to reduction. To prove that the coercion-based reduction rule (39) is equivalent to the threesome rule (23), we need to establish that

\[
\llangle T \Leftarrow S \rrangle \circ \llangle P \Leftarrow S \rrangle \rightarrow \star \llangle T \Leftarrow S \rrangle
\]

To prove this, we need to establish that mapping from coercions back to threesomes is invariant with respect to coercion reduction.

**Lemma 12** (Coercion reduction preserves \(\llangle \rrangle\)). \(, \quad \text{Suppose } c \text{ is well-typed. If } c \rightarrow \star c', \text{then } \llangle c \rrangle = \llangle c' \rrangle\).

**Corollary 2.** \(, \quad \text{If } \llangle T \Leftarrow R \rrangle \circ \llangle R \Leftarrow S \rrangle \rightarrow \star \llangle T \Leftarrow S \rrangle\).

Proof. First, we have \(\llangle T \Leftarrow R \rrangle \circ \llangle R \Leftarrow S \rrangle \rightarrow \llangle T \Leftarrow S \rrangle\). Then because coercion reduction is strongly normalizing, there is a \(c'\) such that \(\llangle T \Leftarrow S \rrangle \circ \llangle R \Leftarrow S \rrangle \rightarrow c'\) and \(\text{nm } c\). Then by Lemma 12 we have \(\llangle c \rrangle = \llangle c' \rrangle\) and therefore \(c' = \llangle T \Leftarrow S \rrangle\).

Putting these results together, we have an isomorphism between the threesome calculus and the coercion-based calculus of Figure 7.

**Theorem 5** (Isomorphism between the threesome calculus and the coercion-based calculus).

1. \(\llangle \rrangle\) is bijective, that is \(\llangle \text{nor} \rrangle = \llangle \text{nor} \rrangle\) if \(\text{nor}\).

2. \(\llangle \rrangle\) is structure (reduction) preserving, that is \(\llangle \text{nor} \rrangle\) if and only if \(\text{nor}\).

3. The correctness of the threesome calculus is a straightforward consequence of these lemmas.

4. Space efficiency from Section 3.2 carries over to the full threesome calculus in a straightforward manner.
6. Related Work

The integration of static and dynamic typing has roots in the
1970’s and 1980’s, with the any type and force expression in
CLU (Liskov et al. 1979) and the Dynamic type and coerce ex-
pression in Amber (Cardelli 1986). Similar constructs appear in
Cedar (Lampson 1983), Modula-2 (Roverne 1986), and Modu-
la-3 (Cardelli et al. 1989). Casts are generalized to typecase in
Modula-2 and 3 their semantics is formalized by Abadi et al. (1989,
1991). In this early work on casts and the Dynamic type, run-time
checks are based on type equality. Thatte (1990) observes that
type equality requires programmers to explicitly reason about the
checks are based on type equality. Thatte (1990) observes that

![Figure 7. Coercion calculus with blame](image)

![Figure 8. Isomorphism between threesomes and coercions](image)
Syntax

terms \( s, t \) ::= k \mid x : S.t \mid s \; t \mid (c) \; s \) where \( mn \; c \)

uncoerced values \( u \) ::= \( k \mid \lambda x : S.t \)

values \( v, w \) ::= \( u \mid (c) \; u \) where \( mn \; c \)

contractums \( r \) ::= \( t \) blame \( l \)

cast-free contexts \( F \) ::= \( [] \mid E[\; t \] \mid E[v \; ] \)

evaluation contexts \( E \) ::= \( F \mid (c) \; E \)

Additional typing rules

\[ \Gamma \vdash s : S \vdash t : T \]

Compile blame calculus to coercion-based calculus

\[ \langle \langle t \rangle \rangle = t \]

\[ \langle \langle k \rangle \rangle = k \]

\[ \langle \lambda x : S.t \rangle = \lambda x : S. \langle \langle t \rangle \rangle \]

\[ \langle \langle t \; s \rangle \rangle = \langle \langle t \rangle \rangle \; \langle \langle s \rangle \rangle \]

Reductions

\[ (\lambda x : S.t) \; v \rightarrow [x := v] \; t \] (35)

\[ k \; k' \rightarrow \delta(k, k') \] (36)

\[ (c \rightarrow d) \; u \rightarrow [d] \; u \; (c) \; w \] (37)

Cast reductions

\[ \langle x \rangle \; u \rightarrow_{c} u \] (38)

\[ \langle d \rangle \; (c) \; s \rightarrow_{c} \; (c') \; s \] if \( d \; c \rightarrow c' \) and \( nm \; c' \) (39)

\[ \langle \text{Fail} \rangle \; T \rightarrow_{S} \; \text{blame} \; l \] (40)

Single-step evaluation

\[ t \rightarrow t' \]

\[ F[t] \rightarrow F[t'] \]

\[ F[t] \rightarrow \text{blame} \; l \]

Figure 9. Coercion-based lambda calculus with blame

respect to \( <_{\text{eq}} \), a positive coercion is an upcast, and a neutral coercion represents failure. We conjecture that a threesome \( (T \overset{R}{\Rightarrow} S) \), where \( R \) does not contain \( \bot \), is equivalent to a cast with factoring \( c^+ \circ c^\circ c^- \) where \( c^- \) is a downcast from \( S \) to \( R \), and \( c^+ \) is the identity coercion on \( R \), and \( c^\circ \) is an upcast from \( R \) to \( T \).

The primary goal of Henglein’s work was to minimize the number of casts inserted during compilation, which explains his use of the \( \psi \)-reduction to remove projection-injection pairs. In contrast, the focus of this paper is on integrating static and dynamic typing, and the boundary between static and dynamic regions require certain run-time checks to maintain the integrity of the static region. To maintain the integrity of the static types, we only use \( \phi \)-reduction. That being said, an interesting direction for future work would be to try and reduce the number of inserted casts using Henglein’s techniques while remaining sound.

Gray et al. (2005) propose adding the type Dynamic to Java and apply the technology of contract checking to casts. Towards formalizing the ideas of Gray et al. (2005), Siek and Taha (2006) and Gronski et al. (2006) generalize Thatte’s up and down-casts to a single cast capable of up, down, and cross casts. Furthermore, Siek and Taha (2006) observe that subtyping is not suitable for statically characterizing casts involving type Dynamic and propose the compatibility relation, written \( \sim \), to fill this role. These generalized casts play an important role in the intermediate languages of gradual typings (Siek and Taha 2006, 2007) and hybrid typing (Gronski et al. 2006, Flanagan 2006, Flanagan et al. 2006).

Tobin-Hochstadt and Felleisen (2006) formalize the interaction between static and dynamic typing at the granularity of modules and develop a precursor to the Blame Theorem. Wadler and Findler (2007, 2009) design the blame calculus, adding blame tracking to the generalized casts of Siek and Taha (2006) and Gronski et al. (2006), drawing on the blame tracking of higher-order contracts (Findler and Felleisen 2002). Wadler and Findler (2009) formulate and prove the Blame Theorem: statically typed regions of a program can’t be blamed for a cast error. Gronski and Flanagan (2007) show that casts with a single blame label are just as expressive as casts with two blame labels or labels with polarity.

Herman et al. (2007) observe that in a straightforward implementation of the generalized casts, there can be unbounded runtime space overhead. To solve this problem, Herman et al. (2007) perform stack inspection to find sequences of casts and use the coercion calculus of Henglein (1994) to compress those sequences. Siek and Taha (2007) describe a partial solution to the space efficiency problem using a merge operator that is a precursor to the merge algorithm given in this paper. Siek et al. (2009) show how to augment the coercion calculus with blame tracking, thereby obtaining a theoretical bound on space consumption for blame calculus implementations.

7. Conclusion

In this paper we present threesomes, a typed-based solution to the space-efficiency problem of higher-order casts. We first present a simplified threesome calculus where sequences of casts are compressed by taking the greatest lower bound with respect to naive subtypng. We prove that the simplified threesome calculus is equivalent to the blame calculus (ignoring blame allocation) and we prove that the simplified threesome calculus is space efficient. We then present the threesome calculus with full support for blame tracking and prove that it is equivalent to the blame calculus. We prove that threesomes are isomorphic to Henglein’s coercions in normal form and that threesome composition is equivalent to coercion composition followed by normalization.

References


Cormac Flanagan, Stephen N. Freund, and Aaron Tomb. Hybrid types, invariants, and refinements for imperative objects. In FOOL/WOOD ‘06:
Appendix

7.1 Correctness of Simplified Threesomes

Proof of Proposition 1. The proof is by strong induction on the sum of the height of S and T.

We define the append operation @ for contexts as follows.

\[ E@\square = E \]
\[ E@E[S]t = (E@E'[S]t) \]
\[ E@E[v]t = (E@E'[v]t) \]

If \( E@F \neq E'[F] \), then

\[ E@F[S]t = (E@F[S]t) \]

Proof of Unique Decomposition 2. The proof is by induction on the typing derivation \( \emptyset \vdash t : T \).

1. \( \emptyset \vdash k : \text{typeof}(k) \) : k is a value.
2. \( \emptyset \vdash x : T \) : vacuously true.
3. \( \emptyset \vdash \lambda x : S. s : \lambda x : S. s \) is a value.
4. \( \emptyset \vdash s : T \rightarrow S \) : \( \emptyset \vdash t : T \) : Either \( s \) is a value, or not.
   - (a) Suppose \( s \) is a value. Either \( t \) is a value, or not.
     - i. Suppose \( t \) is a value. By the canonical forms lemma, \( s \) is either a function or a functional cast. In either case \( s \) is a redex. Furthermore, the only context that decomposes \( s \) into a redex is \( \square \).
     - ii. Suppose \( t \) is not a value. Then we apply the induction hypothesis to get a unique context \( E \) and redex \( t' \) where \( t = E[t'] \). The unique context for \( s \) is therefore \( \square[s]@E \).
   - (b) Suppose \( s \) is not a value. Then we apply the induction hypothesis to get a unique context \( E \) and redex \( s' \) where \( s = E[s'] \). The unique context for \( s \) is therefore \( \square[s]@E \).
5. \( \emptyset \vdash (T \rightarrow S) s : T \) : Either \( s \) is a value, or not.
   - (a) Suppose \( s \) is a value. Then either \( (T \rightarrow S) s \) is also a value or it is a redex. If it is a redex, then the unique context is \( \square \).
   - (b) Suppose \( s \) is not a value. We have two cases to consider.
     - If \( s \) is a cast, then \( (T \rightarrow S) s \) is a redex and the unique context is \( \square \). (Any other context that puts the hole inside \( s \) would contain adjacent casts, which is impossible.)
     - If \( s \) is not a cast, we apply the induction hypothesis to get a unique context \( E \) and redex \( s' \) where \( s = E[s'] \). The unique context for \( (T \rightarrow S) s \) is therefore \( \square[T \rightarrow S]@E \).
     - Because \( s \) is not a cast, the top of \( E \) is not a cast and appending \( \square[T \rightarrow S]@E \) with \( E \) will not result in adjacent casts and therefore produces a well-formed context.

Towards proving the fundamental property of casts, we define the bisimulation relation \( \approx \) by closing the following two rules with respect to contexts. The second rule is necessary for \( \approx \) to be a bisimulation.

\[
\frac{t \approx t'}{T \leftarrow S \approx t} \quad \frac{R \leftarrow S \approx t}{t \approx S \rightarrow t} \quad \frac{t \approx t'}{t \approx S \rightarrow t}
\]

Lemma 13 (Substitution preserves \( \approx \)). If \( s \approx t \) and \( v_i \approx v_i \), then

\[
[x := v_i] s \approx [x := v_i] t.
\]

Proof. The proof is by induction on the derivation of \( s \approx t \).

Lemma 14 (\( \approx \) is a weak bisimulation.). Suppose \( s \approx t \).

1. If \( s \rightarrow r_1 \), then there exists \( r_1 \) where \( t \rightarrow^* r_1 \) and \( r_1 \approx r_1 \).
2. If $t \rightarrow r_z$, then there exists $r_z$ where $s \rightarrow^* r_z$ and $r_z \approx r_z$.

Proof.

1. The proof is by a lengthy case analysis on $s \rightarrow r_z$. The case for function application uses Lemma 13.
2. The proof is by a lengthy case analysis on $t \rightarrow r_z$. The case for function application uses Lemma 13.

Lemma 15. If $s \approx t$, then $s \Downarrow$ if and only if $t \Downarrow$.

Proof.

1. $(\Rightarrow)$ The proof is by induction on the reduction $s \rightarrow^* f$.
   (a) Case $s = f$: From $s \approx t$ and Lemma 14 we have $t \rightarrow^* f'$ and therefore $t \Downarrow$.
   (b) Case $s \rightarrow s'$ and $s' \rightarrow^* f$: From $s \approx t$ and Lemma 14 we have $t \rightarrow^* t'$ with $s' \approx t'$. Then by the induction hypothesis, $t \Downarrow$.
2. $(\Leftarrow)$ The proof is symmetric to the above case.

Lemma 16. If $s \approx t$, then $C[s] \approx C[t]$.

Proof. The proof by induction on $C$.

Lemma 17. If $s \approx t$, then $s =_{\text{ctx}} t$.

Proof. We fix $C$ and need to show that $C[s] \Downarrow$ if and only if $C[t] \Downarrow$. By Lemma 16 we have $C[s] \approx C[t]$. We conclude by applying Lemma 15.

Lemma 18. $t \approx t$.

Proof. By induction on $t$.

Proof of Lemma 2. Assuming $\text{Tk} : S <_{\text{ctx}} R$, we need to show that $(T \leftarrow S) t =_{\text{ctx}} (T \leftarrow R \leftarrow S) t$. We have $t \approx t$ and therefore $(T \leftarrow S) t \approx (T \leftarrow R \leftarrow S) t$. We conclude by Lemma 17.

7.2 Proof of Space Efficiency

Proof of Proposition 3.

1. The proof is a straightforward induction on the type $T$.
2. The proof is by strong induction on the sum of the heights of $S$ and $T$.
3. The proof is by induction on type $T$ with case analysis on $S$.

Proof of Lemma 6. The proof is by inversion on $t \rightarrow t'$ and cases on $\rightarrow$. The case for rule (16) uses Proposition 3 (part 2).

Proof of Lemma 7. The proof is by induction on $t$. The only interesting case is for casts. We have $T <_{\text{ctx}} \{R \Leftarrow S\} s$ and therefore $T <_{\text{ctx}} \{R\}$ and $T <_{\text{ctx}} \{S\}$. Then by Proposition 3 (part 2) we have that $T <_{\text{ctx}} \{R\}kS$. By the induction hypothesis we have $T <_{\text{ctx}} \{s\}$. Therefore $T <_{\text{ctx}} \{RkS\} \{s\}$.

Proof of Theorem 2. First, we have $\&[t] <_{\text{ctx}} [t]$ by Proposition 1. We have $\&[t] <_{\text{ctx}} \{t\}$ by Lemma 7. We then proceed by induction on $\{t\} \rightarrow t'$.
1. In the base case we have $t' = \{t\}$. So $\&[t] <_{\text{ctx}} [t']$ and then by Proposition 3 (part 3) we can conclude that $\text{size}(T) \leq \text{size}(\&[t])$ for any $T$ in $t'$.
2. For the induction step, we have $\{t\} \rightarrow t_1$ and $t_1 \rightarrow t'$. By Lemma 6 we have $\&[t] <_{\text{ctx}} t_1$. Then by the induction hypothesis we have $\&[t] <_{\text{ctx}} t'$. We conclude that $\text{size}(T) \leq \text{size}(\&[t])$ for any $T$ in $t'$ by applying Proposition 3 (part 1 and 3).

7.3 Correctness of Threesomes

Proof of Proposition 5. The proof is by induction on the sum of the heights of $S$ and $T$.

Proof of Proposition 4. The proof is by induction on the sum of the heights of $Q$ and $P$.

Lemma 19. Suppose $s_2 \approx (T \leftarrow^* S) u$. Then $s_2 \rightarrow^* \text{ blame } l$.

Proof of Lemma 8.
1. The proof is by case analysis on $t_2 \rightarrow r_2$.
2. The proof is by case analysis on $t_2 \rightarrow r_2$. In the case $F[(T \leftarrow^* S) u] \rightarrow \text{ blame } l$, we apply Lemma 19 to show that $t_2 \rightarrow^* \text{ blame } l$.

Proof of Lemma 9. The proof is by induction on the term $t$, using rule (24) for relating casts.

Proof of Lemma 19. The proof is by induction on the derivation of $s_2 \approx (T \leftarrow^* S) v$.

Proof of Lemma 10. We need to show that if $t_2 \approx t_3$, then $t_2 \Downarrow$ if and only if $t_3 \Downarrow$.
1. $(\Rightarrow)$ The proof is by induction on the reduction $t_2 \rightarrow^* f_2$.
2. $(\Leftarrow)$ The proof is by induction on the reduction $t_3 \rightarrow^* f_3$.

Proof of Theorem 4. We need to show that $\{t\} \Downarrow$ if $t \Downarrow$. By Lemma 9 we have $t \approx \{t\}$. We conclude by Lemma 10.

7.4 Isomorphism Between Threesomes and Coercions

Proof of Proposition 6.
1. To show that $nm c$ implies $\beta c'$. $c \rightarrow c'$, perform induction on the derivation of $nm c$.
2. We need to show that $\beta c'$. $c \rightarrow c'$ implies $nm c$. Towards a contradiction, we assume $\neg nm c$. We proceed by induction on $c$. Each of the base cases is vacuously true. In the case where $c = c_1 \rightarrow c_2$, we apply the induction hypothesis to get a reduction in $c_1$ or $c_2$ and therefore a contradiction. In the case where $c = c_1 \circ c_2$, there are many cases to consider, but in each case there is a reduction.

Proof of Proposition 7. The proof is by induction on $P$.

Proof of Lemma 11.
1. We prove $\{\{T \leftarrow P\} S\}^{-1} = (T \leftarrow S)$ by induction on $P$.
2. We prove $\{\{t\}^{-1}\} = c$ by induction on the derivation of $c$.

Proof of Lemma 12. The proof is by induction on the reduction sequence, with case analysis on each reduction.

Proof of Theorem 5.
1. The proof of $\{\{t_3\}^{-1}\} = t_3$ is by induction on the typing derivation for $t_3$ and the proof of $\{\{t_3\}^{-1}\} = t_3$ is by induction on the typing derivation of $t_3$.
2. We prove that $t_3 \rightarrow t_3$ if and only if $\{t_3\} \rightarrow \{t_3\}$.
   (a) We show that $t_3 \rightarrow t_3$ implies $\{t_3\} \rightarrow \{t_3\}$. The proof is by cases on reduction, using Corollary 2 for rule (23).
   (b) We show that $\{t_3\} \rightarrow \{t_3\}$ implies $t_3 \rightarrow t_3$. The proof is by cases on reduction, using Corollary 2 for rule (39).