Contracts made manifest*

MICHAEL GREENBERG, BENJAMIN C. PIERCE and STEPHANIE WEIRICH
University of Pennsylvania, Philadelphia, PA 19104, USA
(e-mail: mgree@seas.upenn.edu)

Abstract

Since Findler and Felleisen (Findler, R. B. & Felleisen, M. 2002) introduced higher-order contracts, many variants have been proposed. Broadly, these fall into two groups: some follow Findler and Felleisen (2002) in using latent contracts, purely dynamic checks that are transparent to the type system; others use manifest contracts, where refinement types record the most recent check that has been applied to each value. These two approaches are commonly assumed to be equivalent—different ways of implementing the same idea, one retaining a simple type system, and the other providing more static information. Our goal is to formalize and clarify this folklore understanding. Our work extends that of Gronski and Flanagan (Gronski, J. & Flanagan, C. 2007), who defined a latent calculus $\lambda_C$ and a manifest calculus $\lambda_H$, gave a translation $\phi$ from $\lambda_C$ to $\lambda_H$, and proved that if a $\lambda_C$ term reduces to a constant, so does its $\phi$-image. We enrich their account with a translation $\psi$ from $\lambda_H$ to $\lambda_C$ and prove an analogous theorem. We then generalize the whole framework to dependent contracts, whose predicates can mention free variables. This extension is both pragmatically crucial, supporting a much more interesting range of contracts, and theoretically challenging. We define dependent versions of $\lambda_H$ and two dialects (“lax” and “picky”) of $\lambda_C$, establish type soundness—a substantial result in itself, for $\lambda_H$ – and extend $\phi$ and $\psi$ accordingly. Surprisingly, the intuition that the latent and manifest systems are equivalent now breaks down: the extended translations preserve behavior in one direction, but in the other, sometimes yield terms that blame more.

1 Introduction

The idea of contracts—arbitrary program predicates acting as dynamic pre- and post-conditions—was popularized by Eiffel (Meyer 1992). More recently, Findler and Felleisen (2002) introduced a $\lambda$-calculus with higher-order contracts. This calculus includes terms like $\langle\{x:\text{Int} \mid \text{pos } x\}\rangle^{l,l'}$, in which a boolean predicate, pos, is applied to a run-time value $1$. This term evaluates to $1$, since pos $1$ returns true. On the other hand, the term $\langle\{x:\text{Int} \mid \text{pos } x\}\rangle^{l,l'}$ $0$ evaluates to blame, written $\uparrow l$, signaling that a contract with label $l$ has been violated. The other label on the

contract, \( l' \), comes into play with function contracts, \( c_1 \mapsto c_2 \). For example, the term

\[
\langle \{x : \text{Int} \mid \text{nonzero } x \} \mapsto \{x : \text{Int} \mid \text{pos } x \} \rangle^{l'} (\lambda x : \text{Int}. x - 1)
\]

“wraps” the function \( \lambda x : \text{Int}. x - 1 \) in a pair of checks: whenever the wrapped function is called, the argument is checked to see whether it is nonzero; if not, the blame term \( \uparrow l' \) is produced, signaling that the context of the contracted term violated the expectations of the contract. If the argument check succeeds, then the function is run and its result is checked against the contract. If this fails (e.g., if the wrapped function is applied to 1).

Findler and Felleisen’s work (2002) sparked a resurgence of interest in contracts, and in the intervening years a bewildering variety of related systems has been studied. Broadly, these come in two different sorts. In systems with latent contracts, types and contracts are orthogonal features. Examples of this style include Findler and Felleisen’s original system (2002), Blume and McAllester (2006), Hinze et al. (2006), Chitil and Huch (2007), Guha et al. (2007), and Tobin-Hochstadt and Felleisen (2008). By contrast, manifest contracts are integrated into the type system, which tracks, for each value, the most recently checked contract. Hybrid types (Flanagan 2008) are a well-known example in this style; others include the works of Ou et al. (2004), Knowles et al. (2006), and Wadler and Findler (2009).

A key feature of manifest systems is that descriptions like \( \{x : \text{Int} \mid \text{nonzero } x \} \) are incorporated into the type system as refinement types. Values of refinement type are introduced via casts like \( \langle \{x : \text{Int} \mid \text{true} \} \Rightarrow \{x : \text{Int} \mid \text{nonzero } x \} \rangle^{l} n \), which has static type \( \{x : \text{Int} \mid \text{nonzero } x \} \) and checks, dynamically, that \( n \) really is nonzero, raising \( \uparrow l \) otherwise. Similarly, \( \langle \{x : \text{Int} \mid \text{nonzero } x \} \Rightarrow \{x : \text{Int} \mid \text{pos } x \} \rangle^{l} n \) casts an integer that is statically known to be nonzero to one that is statically known to be positive.

The manifest analogue of function contracts is casts between function types. For example, consider

\[
f = \langle \{x : \text{Int} \Rightarrow \text{Int} \Rightarrow \{x : \text{Int} \mid \text{pos } x \} \Rightarrow \{x : \text{Int} \mid \text{pos } x \} \rangle \ (\lambda x : \text{Int}. x - 1),
\]

where \( \{x : \text{Int} \Rightarrow \text{Int} \Rightarrow \{x : \text{Int} \mid \text{true} \} \} \). The sequence of events when \( f \) is applied to some argument \( n \) (of type \( P \)) is similar to what we saw before:

\[
f \ n \rightarrow_h \langle \{x : \text{Int} \mid \text{pos } x \} \rangle (\langle \{x : \text{Int} \mid \text{true} \} \rangle (\lambda x : \text{Int}. x - 1)) (\langle \{x : \text{Int} \mid \text{pos } x \} \Rightarrow \{x : \text{Int} \Rightarrow \text{Int} \Rightarrow \{x : \text{Int} \mid \text{true} \} \rangle n))
\]

First, \( n \) is cast from \( \{x : \text{Int} \mid \text{pos } x \} \) to \( \{x : \text{Int} \} \) (it happens that in this case the cast cannot fail, since the target predicate is just true, but if it did, it would raise \( \uparrow l \)); then the function body is evaluated; and finally its result is cast from \( \{x : \text{Int} \} \) to \( \{x : \text{Int} \mid \text{pos } x \} \), raising \( \uparrow l \) if this fails. The domain cast is contravariant and the codomain cast is covariant.

One point to note here is that casts in the manifest system have just one label, while contract checks in the latent system have two. This difference is not fundamental to the latent/manifest distinction—both latent and manifest systems can be given more or less rich algebras of blame—but rather a question of the pragmatics of assigning responsibility: contract checks (called obligations in Findler & Felleisen 2002) use two labels, while casts use one. Informally, a function contract check \( \langle c_1 \mapsto c_2 \rangle^{l'} f \)
divides responsibility for \( f \)'s behavior between its body and its environment: the programmer is saying “If \( f \) is ever applied to an argument that does not pass \( c_1 \), I refuse responsibility (\( \uparrow l' \)), whereas if \( f \)'s result for good arguments does not satisfy \( c_2 \), I accept responsibility (\( \uparrow l \)).” In a system with casts, the programmer who writes \( \langle R_1 \rightarrow R_2 \Rightarrow S_1 \rightarrow S_2 \rangle f \) is saying, “Although all I know statically about \( f \) is that its results satisfy \( R_2 \) when it is applied to arguments satisfying \( R_1 \), I assert that it’s okay to use it on arguments satisfying \( S_1 \) (because I believe that \( S_1 \) implies \( R_1 \)) and that its results will always satisfy \( S_2 \) (because \( R_2 \) implies \( S_2 \)).” In the latter case, the programmer is taking responsibility for both assertions (so \( \uparrow l \) makes sense in both cases), while the additional responsibility for checking that arguments satisfy \( S_1 \) will be discharged elsewhere (by another cast, with a different label).

While contract checks in latent systems may seem intuitively to be much the same thing as casts in manifest systems, the formal correspondence is not immediate. How do the contravariant function casts of \( \lambda H \) relate to the invariant checks of \( \lambda C \)? How does \( \lambda H \) model \( \lambda C \)'s pair of polarized blame labels? These questions have led to some confusion in the community about the nature of contracts. Indeed, as we will see, matters become yet murkier in richer languages with features such as dependency.

Gronski and Flanagan (2007) initiated a formal investigation of the connection between the latent and manifest worlds. They defined a core calculus, \( \lambda C \), capturing the essence of latent contracts in a simply typed \( \lambda \)-calculus, and an analogous manifest calculus \( \lambda H \). To compare these systems, they introduced a type-preserving translation \( \phi \) from \( \lambda C \) to \( \lambda H \). What makes \( \phi \) interesting is that it relates the languages feature for feature: contracts over base types are mapped to casts at base type, and function contracts are mapped to function casts. The main result is that \( \phi \) preserves behavior, in the sense that if a term \( t \) in \( \lambda C \) evaluates to a constant \( k \) or blame \( \uparrow l \), then its translation \( \phi(t) \) evaluates similarly.

Our work extends their work in two directions. First, we strengthen their main result by introducing a new feature-for-feature translation \( \psi \) from \( \lambda H \) to \( \lambda C \) and proving a similar correspondence theorem for \( \psi \). (We also give a new, more detailed proof of the correspondence theorem for \( \phi \).) These correspondences show that the manifest and latent approaches are effectively equivalent in the non-dependent case.

Second, and more significantly, we extend the whole story to allow dependent function contracts in \( \lambda C \) and dependent arrow types in \( \lambda H \). Dependency is extremely handy in contracts, as it allows for precise specifications of how the results of functions depend on their arguments. For example, here is a contract that we might use with an implementation of vector concatenation:

\[
z_1 : \text{Vec} \mapsto z_2 : \text{Vec} \mapsto \{ z_3 : \text{Vec} \mid \text{vlen } z_3 = \text{vlen } z_1 + \text{vlen } z_2 \}
\]

Adding dependent contracts to \( \lambda C \) is easy: the dependency is all in the contracts and the types stay simple. We have just one significant design choice: Should domain contracts be rechecked when the bound variable appears the codomain contract? This choice leads to two dialects of \( \lambda C \), one that does recheck (\( \text{picky } \lambda C \)) and another that does not (\( \text{lax } \lambda C \)). The choice is not clear, so we consider both. The question of which blame labels belong on this extra check is discussed at length in Dimoulas et al. (2011), which introduces \( \text{indy} \) blame. Indy blame is a variant of picky. We do
not consider it in depth here, since it does not affect whether or not blame is raised, only which blame. We discuss this point more in Section 7.3. In λH, on the other hand, dependency significantly complicates the metatheory, requiring the addition of a denotational semantics for types and kinds to break a potential circularity in definitions, plus an intricate sequence of technical lemmas involving parallel reduction to establish type soundness.

Surprisingly, the tight correspondence between λC and λH breaks down in the dependent case: the natural generalization of translations does not preserve behavior exactly. Indeed, we can place λH between the two variants of λC on an “axis of blame” (Figure 1), where evaluation behavior is preserved exactly when moving left on the axis (from picky λC to λH to lax λC), but translated terms can blame more than their pre-images when moving right.1 It is still the case that when a pre-image raises blame, its translation blames as well—though not necessarily the same label. The discrepancy arises in the case of “abusive” contracts, such as

\[ f : \{
\{x : \text{Int} \mid \text{nonzero } x\} \mapsto \{y : \text{Int} \mid \text{true}\}\} \mapsto \{z : \text{Int} \mid f \ 0 = 0\} \]

This rather strange contract has the form \( f : c_1 \mapsto c_2 \), where \( c_2 \) uses \( f \) in a way that violates \( c_1 \)!. In particular, if we apply it (in lax λC) to \( \lambda f : \text{Int} \to \text{Int} \). 0 and then apply the result to \( \lambda x : \text{Int} \). x and 5, the final result will be 5, since \( \lambda x : \text{Int} \). x does satisfy the contract \( \{x : \text{Int} \mid \text{nonzero } x\} \mapsto \{y : \text{Int} \mid \text{true}\}\) and 5 satisfies the contract \( \{z : \text{Int} \mid (\lambda x : \text{Int} \). x) 0 = 0\}. However, running the translation of \( f \) in λH yields an extra check, wrapping the occurrence of \( f \) in the codomain contract with a cast from \( \{x : \text{Int} \mid \text{nonzero } x\} \mapsto \{y : \text{Int} \mid \text{true}\}\) to \( \{x : \text{Int} \mid \text{true}\} \mapsto \{y : \text{Int} \mid \text{true}\}\), which fails when the wrapped function is applied to 0. We discuss this phenomenon in greater detail in Section 4.

We should note at the outset that, like Gronski and Flanagan (2007), we are interested in translations that relate λC and λH feature for feature, i.e., mapping base contracts to base contracts and function contracts to function contracts. Translations that do not map feature for feature can give an exact treatment of blame. Consider the following dependent version of the wrap operator from Findler and Felleisen (2002). There are two cases: one for refinements of base types \( B \), another for

\[ f : \{
\{x : B \mid \text{nonzero } x\} \mapsto \{y : B \mid \text{true}\}\} \mapsto \{z : B \mid f \ 0 = 0\} \]

1 There might, in principle, be some other way of defining \( \phi \) and \( \psi \) that (a) preserves types, (b) maps feature for feature, and (c) induces an exact behavioral equivalence. After considering a number of alternatives, we conjecture that no such \( \phi \) and \( \psi \) exist.
dependent function contracts
\[
\phi((\{x:B \mid t\})^{\mathcal{J}/}) = ([B] \Rightarrow \{x:B \mid \phi(t)\})^\mathcal{J}
\]
\[
\phi((x : c_1 \mapsto c_2)^{\mathcal{J}/}) = \lambda f : [x : c_1 \mapsto c_2].
\]
\[
\lambda x : [c_1].
\]
\[
\phi((c_2)^{\mathcal{J}/}) (f (\phi((c_1)^{\mathcal{J}/}) x))
\]

We can define a similar mapping function that implements \(\lambda_H\)'s semantics as base-type contracts in lax or picky \(\lambda_C\). It is unsurprising that an exact mapping exists: \(\lambda_C\) and \(\lambda_H\) are lambda calculi that feature, among other things, a way to conditionally raise exceptions. That these languages are inter-encodable is completely unsurprising. But translations like these do not relate function contracts to function casts at all, so they do not do much to tell us about how semantics of contracts and that of casts relate.

In summary, our main contributions are (a) the translation \(\psi\) and a symmetric version of Gronski and Flanagan’s behavioral correspondence theorem (2007), (b) the basic metatheory of (call-by-value (CBV), blame-sensitive) dependent \(\lambda_H\), (c) dependent versions of \(\phi\) and \(\psi\), and their properties with regard to \(\lambda_H\) and both dialects of \(\lambda_C\), and (d) a weaker behavioral correspondence in the dependent case. We restrict ourselves to strongly normalizing programs, though we believe the results should generalize readily to programs with recursion and nontermination. This paper extends the discussion of Greenberg et al. (2010), giving more interesting proofs.

2 The non-dependent languages

We begin in this section by defining the non-dependent versions of \(\lambda_C\) and \(\lambda_H\) and continue in Section 3 with the translations between them. The dependent languages, dependent translations, and their properties are developed in Sections 4, 6, and 7. Throughout the paper, rules prefixed with an E or an F are operational rules for \(\lambda_C\) and \(\lambda_H\), respectively. An initial T is used for \(\lambda_C\) typing rules; typing rules beginning with an S belong to \(\lambda_H\).

All of our languages will share a set of base types and first-order constants, given in Figure 2. Let the set \(\mathcal{K}\) contain constants of base type \(B\). We assume that \(\text{Bool}\) is among the base types, with \(\mathcal{K}_\text{Bool} = \{\text{true}, \text{false}\}\).

2.1 The language \(\lambda_C\)

The language \(\lambda_C\) is the simply typed \(\lambda\)-calculus straightforwardly augmented with contracts. Contracts \(c\) come in two forms: base contracts \(\{x:B \mid t\}\) over a base type \(B\), and higher-order contracts \(c_1 \mapsto c_2\), which check the arguments and results of functions. We can use contracts in terms with the contract obligation \(\langle c \rangle^{\mathcal{J}/}\). Applying
a contract obligation \(\langle c \rangle^{l'}\) to a term \(t\) dynamically ensures that \(t\) and its surrounding context satisfy \(c\). If \(t\) does not satisfy \(c\), then the positive label \(l\) will be blamed and the whole term will reduce to \(\uparrow l\); on the other hand, if the context does not treat \(\langle c \rangle^{l'} t\) as \(c\) demands, then the negative label \(l'\) will be blamed and the term will reduce to \(\uparrow l'\). In contexts where it is unambiguous, we refer to contract obligations simply as contracts.

The syntax and semantics of \(\lambda_C\) appear in Figure 3, with some common definitions (shared with \(\lambda_H\)) in Figure 2. Besides the contract term \(\langle c \rangle^{l'}\), \(\lambda_C\) includes first-order
Contracts made manifest

231

constants \(k\), blame, and active checks \(\{x:B \mid t_1\}, t_2, k\}^l\). Active checks do not appear in source programs; they are a technical artifact of the small-step operational semantics, as we explain below. Also, note that we only allow contracts over base types \(B\): we have function contracts, like \(\{x:\text{Int} \mid \text{pos } x\} \mapsto \{x:\text{Int} \mid \text{nonzero } x\}\), but not base contracts over functions themselves, like \(\{f:\text{Bool} \rightarrow \text{Bool} \mid f \text{ true } = f \text{ false}\}\).

Values \(v\) include constants, abstractions, contracts, and function contracts applied to values (more on these later); a result \(r\) is either a value or \(\uparrow l\) for some \(l\).

We interpret constants using two constructions: the type-assignment function \(\text{ty}_c\), which maps constants to first-order types of the form \(B_1 \rightarrow B_2 \rightarrow \ldots \rightarrow B_n\) (and which is assumed to agree with \(\mathcal{K}_B\)); and the denotation function \(\llbracket - \rrbracket\), which maps constants to functions from constants to constants (or blame, to allow for partiality). Denotations must agree with \(\text{ty}_c\), i.e., if \(\text{ty}_c(k) = B_1 \rightarrow B_2\), then \(\llbracket k \rrbracket(k_1) \in \mathcal{K}_{B_2}\) if \(k_1 \in \mathcal{K}_{B_1}\).

The operational semantics is given in Figure 3. It includes six rules for basic (small-step, CBV) reductions, plus two rules that involve evaluation contexts \(E\) (Figure 3). The evaluation contexts implement left-to-right evaluation for function application. If \(\uparrow l\) appears in the active position of an evaluation context, it is propagated to the top level, like an uncatchable exception. As usual, values (and results) do not step.

The first two basic rules are standard, implementing primitive reductions and \(\beta\)-reductions for abstractions. In these rules, arguments must be values \(v\). Since constants are of first order, we know that when \(E\text{_CONST}\) reduces a well-typed application, the argument is not just a value but a constant.

The rules \(E\text{_CCHECK}, E\text{_OK}, E\text{_FAIL},\) and \(E\text{_CDECOMP}\) describe the semantics of contracts. In \(E\text{_CCHECK}\), base-type contracts applied to constants step to an active check. Active checks include the original contract, the current state of the check, the constant being checked, and a label to blame if necessary. We hold on to the original contract as a technical device for the translation \(\phi\) from \(\lambda_C\) to \(\lambda_H\), since \(\lambda_H\) needs to know the target type of an active check. If the check evaluates to true, then \(E\text{_OK}\) returns the initial constant. If \text{false}, the check has failed and a contract has been violated, so \(E\text{_FAIL}\) steps the term to \(\uparrow l\). Higher-order contracts on a value \(v\) wait to be applied to an additional argument. That is why function contracts applied to values are values. There is no substantial difference between this approach and expanding function contracts into new lambdas. When that argument has also been reduced to a value \(v'\), \(E\text{_CDECOMP}\) decomposes the function cast: The argument value is checked with the argument part of the contract (switching positive and negative blame, since the context is responsible for the argument), and the result of the application is checked with the result contract.

The typing rules for \(\lambda_C\) (Figure 3) are mostly standard. We give types to constants using the type-assignment function \(\text{ty}_c\). Blame expressions have all types. Contracts are checked for well-formedness using the judgment \(\vdash c : T\), comprising the rules \(T\_BASEC\), which require that the checking term in a base contract returns a boolean value when supplied with a term of the right type, and \(T\_FUNC\). Note that the predicate \(t\) in a contract \(\{x:B \mid t\}\) can contain at most \(x\) free, since we
are considering only non-dependent contracts for now. Contract application, like function application, is checked using T_App.

The T_Checking rule only applies in the empty context (active checks are only created at the top level during evaluation). The rule ensures that the contract \( \{x:B \mid t_1\} \) has the right base type for the constant \( k \), the check expression \( t_2 \) has a boolean type, and the check is actually checking the right contract. The latter condition is formalized by the implication: \( t_2 \longrightarrow^* \text{true} \) implies \( t_1[x := k] \longrightarrow^* \text{true} \). True asserts that if \( t_2 \) evaluates to true, then the original check \( t_1[x := k] \) must also evaluate to true. This requirement is needed for two reasons: first, nonsensical terms like \( \langle \{x:\text{Int} \mid \text{pos} \ x\}, \text{true}, 0 \rangle \) should not be well typed; and second, we use this property in showing that the translations are type-preserving (see Section 6). This rule obviously makes type checking for the full “internal language” with checks undecidable, but excluding checks decidability. We could give a more precise condition—for example, that \( t_1[x := k] \longrightarrow^* t_2 \)—but there is no need.

The language enjoys standard preservation and progress theorems. Together, these ensure that evaluating a well-typed term to a normal form always yields a result \( r \), which is either blame or a value.

### 2.2 The language \( \lambda_H \)

Our second core calculus, non-dependent \( \lambda_H \), extends the simply typed \( \lambda \)-calculus with refinement types and cast expressions. The definitions appear in Figure 4. Unlike \( \lambda_C \), which separates contracts from types, \( \lambda_H \) combines them into refined base types \( \{x:B \mid s_1\} \) and function types \( S_1 \rightarrow S_2 \). As for \( \lambda_C \), we do not allow refinement types over functions, nor do we allow refinements of refinements. (Belo et al., 2011 add these features to a dependent \( \lambda_H \).) Unrefined base types \( B \) are not valid types; they must be wrapped in a trivial refinement, as the raw type \( \{x:B \mid \text{true}\} \). The terms of the language are mostly standard, including variables, the same first-order constants as \( \lambda_C \), blame, abstractions, and applications. The cast expression \( (S_1 \Rightarrow S_2)^l \) dynamically checks that a term of type \( S_1 \) can be given type \( S_2 \). Like \( \lambda_C \), active checks are used to give a small-step semantics to cast expressions.

The values of \( \lambda_H \) include constants, abstractions, casts, and function casts applied to values. Results are either values or blame. We give meaning to constants as we did in \( \lambda_C \), reusing \([\_\_\_\_\_]\). Type assignment is via \( \text{ty}_h \), which we assume produces well-formed types (defined in Figure 4). To keep the languages in sync, we require that \( \text{ty}_h \) and \( \text{ty}_c \) agree on “type skeletons”: if \( \text{ty}_c(k) = B_1 \rightarrow B_2 \), then \( \text{ty}_h(k) = \{x:B_1 \mid s_1\} \rightarrow \{x:B_2 \mid s_2\} \).

The small-step, CBV semantics in Figure 4 comprises six basic rules and two rules involving evaluation contexts \( F \). Each rule corresponds closely to its \( \lambda_C \) counterpart.

Notice how the decomposition rules compare. In \( \lambda_C \), the term \( (c_1 \mapsto c_2)^l \ f \ v \) decomposes into two contract checks: \( c_1 \) checks the argument \( v \), and \( c_2 \) checks the result of the application. In \( \lambda_H \) the term \( (S_{11} \rightarrow S_{12} \Rightarrow S_{21} \rightarrow S_{22})^l \ w \) decomposes into two casts: a contravariant cast on the argument and a covariant cast on the result. The contravariant cast \( (S_{21} \Rightarrow S_{11})^l \ w \) makes \( w \) a suitable input for \( w \), while \( (S_{12} \Rightarrow S_{22})^l \) casts the result from \( w \) applied to (the cast) \( w \). Suppose
Fig. 4. Syntax and semantics for $\lambda_H$
\(S_{21} = \{x : \text{Int} \mid \text{pos } x\}\) and \(S_{11} = \{x : B \mid \text{nonzero } x\}\). Then the check on the argument ensures that \(\text{nonzero } x \rightarrow^*_h \text{true}\)—not, as one might expect, that \(\text{pos } w' \rightarrow^*_h \text{true}\). While it is easy to read off from a \(\lambda_C\) contract exactly which checks will occur at runtime, a \(\lambda_H\) cast must be carefully inspected to see exactly which checks will take place. On the other hand, which label will be blamed is clearer with casts—there’s only one!

The typing rules for \(\lambda_H\) (Figure 4) are also similar to those of \(\lambda_C\). Just as the \(\lambda_C\) rule \(T_{\text{Contract}}\) checks to make sure that the contract has the right form, the \(\lambda_H\) rule \(S_{\text{Cast}}\) ensures that the two types in a cast are well formed and have the same simple-type skeleton, defined as \([\_] : S \rightarrow T\) (pronounced “erase \(S\)”):

\[
\begin{align*}
\{ [x : B \mid s] \} &= B \\
[S_1 \rightarrow S_2] &= [S_1] \rightarrow [S_2]
\end{align*}
\]

This prevents “stupid” casts, like \(\langle \lceil \text{Int} \rceil \Rightarrow \lceil \text{Bool} \rceil \rangle\). We define a similar operator, \(\rceil - \rceil : S \rightarrow S\) (pronounced “raw \(S\)”), which trivializes all refinements:

\[
\begin{align*}
\{ [x : B \mid s] \} &= \{ x : B \mid \text{true} \} \\
[S_1 \rightarrow S_2] &= [S_1] \rightarrow [S_2]
\end{align*}
\]

These operations apply to \(\lambda_C\) contracts and types in the natural way. Type well-formedness in \(\lambda_H\) is similar to contract well-formedness in \(\lambda_C\), though the SWF_RAW case needs to be added to get things off the ground.

The active check rule \(S_{\text{Checking}}\) plays a role analogous to the \(T_{\text{Checking}}\) rule in \(\lambda_C\), again using an implication to guarantee that we only have sensible terms in the predicate position. Note that we retain the target type in the active check, and that \(S_{\text{Checking}}\) gives active checks that type—technical moves necessary for preservation.

An important difference is that \(\lambda_H\) has subtyping. The \(S_{\text{Sub}}\) rule allows an expression to be promoted to any well-formed supertype. Refinement types are supertypes if, for all constants of the base type, their condition evaluates to true whenever the subtype’s condition evaluates to true. For function types, we use the standard contravariant subtyping rule. We do not consider source programs with subtyping, since subtyping makes type checking undecidable\(^2\); subtyping is just a technical device for ensuring type preservation. Consider the following reduction:

\[
\langle \{ x : \text{Int} \mid \text{true} \} \Rightarrow \{ x : \text{Int} \mid \text{pos } x \} \rangle^f \ 1 \rightarrow^*_h 1
\]

The source term is well typed at \(\{ x : \text{Int} \mid \text{pos } x \}\). Since it evaluates to 1, we would like to have \(\Delta \vdash 1 : \{ x : \text{Int} \mid \text{pos } x \}\). To have type preservation in general, though, \(\text{ty}_h(1)\) must be a subtype of \(\{ x : \text{Int} \mid s \}\) whenever \(s\{x := 1\} \rightarrow^*_h \text{true}\). That is, constants of base type must have “most-specific” types. One way to satisfy this requirement is to set \(\text{ty}_h(k) = \{ x : B \mid x = k \}\) for \(k \in \mathcal{X}_B\); then if \(s\{x := k\} \rightarrow^*_h \text{true}\), we have \(\vdash \text{ty}_h(k) \ll \{ x : B \mid s \}\). This approach is taken in Ou et al. (2004) and Knowles and Flanagan (2010).

Standard progress and preservation theorems hold for \( \lambda_H \). We can also obtain a semantic type soundness theorem as a restriction of the one for dependent \( \lambda_H \) (Theorem 4.12).

3 The non-dependent translations

The latent and manifest calculi differ in a few respects. Obviously, \( \lambda_C \) uses contract application and \( \lambda_H \) uses casts. Second, \( \lambda_C \) contracts have two labels—positive and negative—where \( \lambda_H \) contracts have a single label. Finally, \( \lambda_H \) has a much richer type system than \( \lambda_C \). Our \( \psi \) from \( \lambda_H \) to \( \lambda_C \) and Gronski and Flanagan’s \( \phi \) (2007) from \( \lambda_C \) to \( \lambda_H \) must account for these differences while carefully mapping “feature for feature.”

The interesting parts of the translations deal with contracts and casts. Everything else is translated homomorphically, though the type annotation on lambdas must be chosen carefully. The full definitions of these translations are in Section 6; the non-dependent definitions are a straightforward restriction.

For \( \psi \), translating from \( \lambda_H \)’s rich types to \( \lambda_C \)’s simple types is easy: we just erase the types to their simple skeletons. The interesting case is translating the cast \( \langle S_1 \Rightarrow S_2 \rangle_L \) to a contract by translating the pair of types together, \( \langle \psi(S_1, S_2) \rangle_L \). We define \( \psi \) as two mutually recursive functions: \( \psi(s) \) translates \( \lambda_H \) terms to \( \lambda_C \) terms; \( \psi(S_1, S_2) \) translates a pair of \( \lambda_H \) types—effectively, a cast—to a \( \lambda_C \) contract. The latter function is defined as follows:

\[
\psi(\{x : B | s_1\}, \{x : B | s_2\}) = \{x : B | \psi(s_2)\}
\]

\[
\psi(S_{11} \to S_{12}, S_{21} \to S_{22}) = \psi(S_{21}, S_{11}) \mapsto \psi(S_{12}, S_{22})
\]

We use single label on the cast in both positive and negative positions of the resulting contract, i.e.:

\[
\psi(\langle S_1 \Rightarrow S_2 \rangle_L) = \langle \psi(S_1, S_2) \rangle_L.
\]

When we translate a pair of refinement types, we produce a contract that will check the predicate of the target type (like \( \text{F.CCHECK} \)); when translating a pair of function types, we translate the domain contravariantly (like \( \text{F.CDECOMP} \)). For example,

\[
\langle \{x : \text{Int} | \text{nonzero } x \} \to \{\text{Int} \Rightarrow \{\text{Int} \to \{y : \text{Int} | \text{pos } y\}\}\}\rangle_L
\]

translates to \( \langle \{x : \text{Int} | \text{nonzero } x \} \mapsto \{y : \text{Int} | \text{pos } y\}\rangle_L \).

Translating from \( \lambda_C \) to \( \lambda_H \), we are moving from a simple type system to a rich one. The translation \( \phi \) (essentially the same as Gronski & Flanagan’s translation (2007)) generates terms in \( \lambda_H \) with raw types—\( \lambda_H \) types with trivial refinements, corresponding to \( \lambda_C \)’s simple types. Since the translation targets raw types, the type preservation theorem is stated as “if \( \Gamma \vdash t : T \) then \( [\Gamma] \vdash \phi(t) : [T] \)” (see Section 7.1).

Whereas the difficulty with \( \psi \) is ensuring that the checks match up, the difficulty with \( \phi \) is ensuring that the terms in \( \lambda_C \) and \( \lambda_H \) will blame the same labels. We deal with this problem by translating a single contract with two blame labels into two separate casts. Intuitively, the cast carrying the negative blame label will run all
of the checks in negative positions in the contract, while the cast with the positive blame label will run the positive checks. We let
\[ \phi(\langle c \rangle_l, l') = \lambda x: \lceil c \rceil . \langle \phi(c) \Rightarrow \lceil c \rceil \rangle_l x, \]
where the translation of contracts to refined types is
\[ \phi(\{ x : B \mid t \}) = \{ x : B \mid \phi(t) \} \]
\[ \phi(c_1 \mapsto c_2) = \phi(c_1) \rightarrow \phi(c_2) \]
The operation of casting into and out of raw types is a kind of “bulletproofing.” Bulletproofing maintains the raw-type invariant: the positive cast takes the argument out of \( \lceil c \rceil \) and the negative cast returns it there. For example,
\[ \langle \{ x : \text{Int} \mid \text{nonzero} \} \mapsto \{ y : \text{Int} \mid \text{pos} \} \rangle_l \]
translates to the \( \lambda_H \) term
\[ \lambda f : [\text{Int} \rightarrow \text{Int}]. \]
\[ \langle \{ x : \text{Int} \mid \text{nonzero} \} \mapsto \{ y : \text{Int} \mid \text{pos} \} \Rightarrow [\text{Int} \rightarrow \text{Int}] \rangle_l f. \]
Unfolding the domain parts of the casts on \( f \), the domain of the negative cast ensures that \( f \)'s argument is nonzero with \( [\text{Int}] \Rightarrow \{ x : \text{Int} \mid \text{nonzero} \} \rangle_l \); the domain of the positive cast does nothing, since \( \langle \{ x : \text{Int} \mid \text{nonzero} \} \Rightarrow [\text{Int}] \rangle_l \) has no effect. Similarly, the codomain of the negative cast does nothing, while the codomain of the positive cast checks that the result is positive. Separating the checks allows \( \lambda_H \) to keep track of blame labels, mimicking \( \lambda_C \). Put more generally, in the positive cast, the positive positions may fail because they are “down casts,” whereas the negative positions are “up casts,” so they cannot fail. The opposite is true for the negative cast. This embodies the idea of contracts as pairs of projections (Findler & Blume 2006). Note that bulletproofing is “overkill” at base type: for example, \( \langle \{ x : \text{Int} \mid \text{nonzero} \} \rangle_l \) translates to
\[ \lambda x : [\text{Int}]. \]
\[ \langle \{ x : \text{Int} \mid \text{nonzero} \} \Rightarrow [\text{Int}] \rangle_l x. \]
Only the positive cast does anything—the negative cast into \([\text{Int}]\) always succeeds. This asymmetry is consistent with \( \lambda_C \), where base-type contracts also ignore the negative label. In Section 4 we extend the bulletproofing translation to dependent contracts—one of our main contributions.

Both \( \phi \) and \( \psi \) preserve behavior in a strong sense: If \( \Gamma \vdash t : B \), then either \( t \) and \( \phi(t) \) both evaluate to the same constant \( k \) or they both raise \( \uparrow l \) for the same \( l \); and conversely for \( \psi \). Interestingly, we need to set up this behavioral correspondence before we can prove that the translations preserve well-typedness because of the T_CHECKING and S_CHECKING rules.
4 The dependent languages

We now extend $\lambda_C$ to dependent function contracts and $\lambda_H$ to dependent functions. Very little needs to be changed in $\lambda_C$, since contracts and types barely interact; the changes to $E_{C\text{Decomp}}$ and $T_{\text{Func}}$ are the important ones. Adding dependency to $\lambda_H$ is more involved. In particular, adding contexts to the subtyping judgment entails adding contexts to $SSUB_{\text{Refine}}$. To avoid a dangerous circularity, we define closing substitutions in terms of a separate type semantics. In addition, the new $F_{C\text{Decomp}}$ rule has a slightly tricky (but necessary) asymmetry, as explained below.

4.1 Dependent $\lambda_C$

Dependent $\lambda_C$ has been studied since Findler and Felleisen (2002); it received a very thorough treatment (with an untyped host language) in Blume and McAllester (2006), was ported to Haskell by Hinze et al. (2006) and Chitil and Huch (2007), and was used as a specification language in Xu et al. (2009). Type soundness is not particularly difficult, since types and contracts are kept separate. Our formulation follows Findler and Felleisen (2002), with a few technical changes to make the proofs for $\phi$ easier.

We have marked the changed rules with a • next to their names. The new $T_{\text{RefineC}}$, $T_{\text{Func}}$, and $E_{C\text{Decomp}}$ rules in Figure 5 suffice to add dependency to $\lambda_C$. To help us work with the translations, we also make some small changes to the bindings in contexts, adding a new binding form to track the labels on a contract check throughout the contract well-formedness judgment. Note that $T_{\text{Func}}$ adds $x : c_1[l']$ to the context when checking the codomain of a function contract, swapping blame labels. We add a new variable rule, $T_{\text{VarC}}$, that treats $x : c[l']$ as if it were its skeleton, $x : [c]$. While unnecessary for $\lambda_C$’s metatheory, this new binding form helps $\phi$ preserve types when translating from $\lambda_H$ to picky $\lambda_C$; see Section 7.1.

Two different variants of the $E_{C\text{Decomp}}$ rule can be found in the literature: they are lax and picky. The original rule in Findler and Felleisen (2002) is lax (like most other contract calculi): it does not recheck $c_1$ when substituting $v'$ into $c_2$. Blume and McAllester (2006) used a picky semantics without observing their departure from Findler and Felleisen (2002); Hinze et al. (2006) choose to be picky as well, substituting $\langle c_1 \rangle[l']$ $v'$ into $c_2$ because it makes their conjunction contract idempotent. We can show (straightforwardly) that both enjoy standard progress and preservation properties. Below, we consider translations to and from both dialects of $\lambda_C$: picky $\lambda_C$ using only $E_{C\text{DecompPicky}}$ in Sections 6.1 and 7.2, and lax $\lambda_C$ using only $E_{C\text{DecompLax}}$ in Sections 6.2 and 7.1. Accordingly, we give two sets of evaluation rules: $\rightarrow_{\text{lax}}$ and $\rightarrow_{\text{picky}}$. When we write $\rightarrow_c$, the metavariable $c$ ranges over picky and lax. We complete the type soundness proofs here generically, writing $\rightarrow$, for the evaluation relation. For the translations in Section 4.2, we specify the evaluation relation that we use.

We make a standard assumption about constant denotations being well typed: if $\Gamma \vdash k \ v : T$ then $\Gamma \vdash \llbracket k \rrbracket(v) : T$. 

https://doi.org/10.1017/S0956796812000135 Published online by Cambridge University Press
Syntax for dependent $\lambda_C$

\[
T ::= B \mid T_1 \rightarrow T_2
\]
\[
c ::= \{x:B \mid t\} \mid x : c_1 \mapsto c_2
\]
\[
\Gamma ::= \emptyset \mid \Gamma, x : T \mid \Gamma, x : c_1 \mapsto c_2
\]
\[
t ::= x \mid k \mid \lambda x : T_1, t_2 \mid t_1 t_2 \mid \emptyset l \mid \langle c\rangle_{l'}^l \mid \langle\{x:B \mid t_1\}, t_2, k\rangle_l
\]
\[
v ::= k \mid \lambda x : T_1, t_2 \mid \langle c\rangle_{l'}^l \mid \langle x : c_1 \mapsto c_2 \rangle_{l'}^l v
\]
\[
r ::= v \mid \emptyset l
\]
\[
E ::= \emptyset t \mid v \mid \langle\{x:B \mid t\}, [], k\rangle_l
\]

Operational semantics for $\lambda_C$

\[
(\lambda x : T_1, t_2) v \longrightarrow_c t_2\{x := v\}
\]
\[
k v \longrightarrow_c \langle k \rangle_l(v)
\]
\[
\langle\{x:B \mid t\}\rangle_{l'}^l k \longrightarrow_c \langle\{x:B \mid t\}, t\{x := k\}, k\rangle_l
\]
\[
⟨x : c_1 \mapsto c_2⟩_{l'}^l v \longrightarrow_{lax} \langle c_2\{x := v\}\rangle_{l'}^l (v (⟨c_1⟩_{l'}^l v'))
\]
\[
⟨x : c_1 \mapsto c_2⟩_{l'}^l v \longrightarrow_{picky} \langle c_2\{x := ⟨c_1⟩_{l'}^l v\}\rangle_{l'}^l (v (⟨c_1⟩_{l'}^l v'))
\]
\[
\langle\{x:B \mid t\}, true, k\rangle_l \longrightarrow_c k
\]
\[
\langle\{x:B \mid t\}, false, k\rangle_l \longrightarrow_c \emptyset l
\]
\[
E[\emptyset l] \longrightarrow_c \emptyset l
\]
\[
E[t_1] \longrightarrow_c E[t_2] \text{ when } t_1 \longrightarrow_c t_2
\]

Contract erasure

\[
\langle\{x:B \mid t\}\rangle_l = B \quad [x : c_1 \mapsto c_2] = [c_1] \rightarrow [c_2]
\]

Typing rules for dependent $\lambda_C$

\[
\Gamma \vdash \Gamma
\]

\[
\vdash \emptyset \quad \text{T_EMPTY}
\]
\[
\vdash \Gamma, c : T \quad \text{T_EXTVAR}\Gamma
\]
\[
\vdash \Gamma, x : T \quad \text{T_EXTVAR}\Gamma
\]

\[
\vdash \Gamma, x : T
\]

\[
\frac{x:T \in \Gamma}{\Gamma \vdash x : T} \quad \text{T_VAR}\Gamma
\]
\[
\frac{x : c_1 \mapsto c_2 \in \Gamma}{\Gamma \vdash x : c_1 \mapsto c_2} \quad \text{T_VAR^C}\Gamma
\]

\[
\frac{\Gamma, x : T \vdash t_1 : T_1}{\Gamma \vdash \lambda x : T_1, t_2 : T_2 \rightarrow T_2} \quad \text{T_LAM}
\]

\[
\frac{\Gamma, x : T \vdash t_1 : T_1, t_2 : T_2}{\Gamma \vdash \Gamma, x : T \vdash t_1 \rightarrow t_2} \quad \text{T_APP}
\]

\[
\frac{\Gamma, \langle c\rangle_{l'}^l k \vdash : T}{\Gamma \vdash \langle c\rangle_{l'}^l : T} \quad \text{T_CONTRACT}\Gamma
\]

\[
\frac{\Gamma \vdash c : T \quad \emptyset \vdash k : B \quad \emptyset \vdash t_2 : T \quad \emptyset \vdash \{\{x:B \mid t_1\}\} : B}{\Gamma \vdash \langle\{x:B \mid t_1\}, t_2, k\rangle_l : B} \quad \text{T_CHECKING}\Gamma
\]

\[
\frac{\Gamma \vdash \langle\{x:B\}_1\}_2 \vdash c : T}{\Gamma \vdash \langle\{x:B\}_1\}_2 \vdash c : T} \quad \text{T_REFINE}\Gamma
\]

\[
\frac{\Gamma \vdash c_1 : T_1 \quad \Gamma, x : c_1 \mapsto c_2 \vdash : T_2}{\Gamma \vdash \Gamma, x : c_1 \mapsto c_2 : T_1 \rightarrow T_2} \quad \text{T_FUNC}\Gamma
\]

Fig. 5. Syntax and semantics for dependent $\lambda_C$.  

https://doi.org/10.1017/S0956796812000135 Published online by Cambridge University Press
4.1 Theorem [Progress]: If $\emptyset \vdash t : T$ then either $t \rightarrow_c t'$ or $t = r$ (i.e., $t = v$ or $t = \uparrow l$).

Proof
By induction on the typing derivation.

For preservation, we prove confluence and substitution lemmas. Note that our substitution lemma must now also cover contracts, since they are no longer closed.

4.2 Lemma [Determinacy]: Let $\rightarrow_c$ be either $\rightarrow_p$ or $\rightarrow_l$. If $t \rightarrow_c t'$ and $t \rightarrow_c t''$, then $t' = t''$.

4.3 Corollary [Coevaluation]: If $\rightarrow_c$ be either $\rightarrow_p$ or $\rightarrow_l$. If $t \rightarrow_c r$ and $t \rightarrow_c t'$, then $t' \rightarrow_c r$.

4.4 Lemma [Term and contract substitution]: If $\emptyset \vdash v : T'$, then

1. if $\Gamma, x : T', \Gamma' \vdash t : T$, then $\Gamma, \Gamma' \{ x := v \} \vdash t \{ x := v \} : T$, and
2. if $\Gamma, x : T', \Gamma' \vdash \llbracket c \rrbracket : T$, then $\Gamma, \Gamma' \{ x := v \} \vdash \llbracket c \rrbracket \{ x := v \} : T$.

Proof
By mutual induction on the typing derivations for $t$ and $c$.

We omit the proof for $x : \llbracket c \rrbracket$ bindings, which is similar.

4.5 Theorem [Preservation]: If $\emptyset \vdash t : T$ and $t \rightarrow_c t'$ then $\emptyset \vdash t' : T$.

Proof
By induction on the typing derivation. This proof is straightforward because typing and contracts hardly interact.

4.2 Dependent $\lambda_H$

Now we come to the challenging part: Dependent $\lambda_H$ and its proof of type soundness. These results require the most complex metatheory in the paper because we need some strong properties about CBV evaluation. The full definitions are in Figures 6 and 7. As before, we have marked the changed rules with a • next to their names.

We enrich the type system with dependent function types, $x : S_1 \rightarrow S_2$, where $x$ may appear in $S_2$. The $S_{\text{Cast}}$ rule and the proofs need a notion of type erasure, $\llbracket S \rrbracket$; type height $|S|$ will also be used in the proofs.

\[
\begin{align*}
\llbracket \_ \rrbracket : S &\rightarrow T & \text{| - |} : S &\rightarrow \mathbb{N} \\
\llbracket \{ x : B \mid s \} \rrbracket &= B & \llbracket \{ x : B \mid s \} \rrbracket &= 1 \\
\llbracket x : S_1 \rightarrow S_2 \rrbracket &= \llbracket S_1 \rrbracket \rightarrow \llbracket S_2 \rrbracket & \llbracket x : S_1 \rightarrow S_2 \rrbracket &= 1 + |S_1| + |S_2| \\
\end{align*}
\]

A new dependent application rule, $S_{\text{APP}}$, substitutes the argument into the result type of the application. We generalize $\text{SWF}_\text{REFINE}$ to allow refinement-type

\footnote{The benefit of a CBV semantics is a better treatment of blame. By contrast, Knowles and Flanagan (2010) cannot treat failed casts as exceptions because that would destroy confluence. They treat them as stuck terms. Readers familiar with the soundness proof of Knowles and Flanagan will notice that our proof is significantly different from their proof. We discuss this in Section 8.}
predicates that use variables from the enclosing context. SWF_Fun adds the bound variable to the context when checking the codomain of function types. In SSub_Fun, subtyping for dependent function types remains contravariant, but we also add the argument variable to the context with the smaller type. This is similar to the function subtyping rule of F_<: (Cardelli et al. 1994).

We need to be careful when implementing higher-order dependent casts in the rule F_CDECOMP. As the cast decomposes, the variables in the codomain types of such a cast must be replaced. However, this substitution is asymmetric; on one side, we cast the argument and on the other we do not. This behavior is required for type soundness. For, suppose we have \( \Delta \vdash x : S_{11} \rightarrow S_{12} \) and \( \Delta \vdash x : S_{21} \rightarrow S_{22} \) with equal skeletons, and values \( \Delta \vdash w : (x : S_{11} \rightarrow S_{12}) \) and \( \Delta \vdash w' : S_{21} \). Then \( \Delta \vdash ((x : S_{11} \rightarrow S_{12}) \Rightarrow x : S_{21} \rightarrow S_{22}) \vdash w) w' : S_{22}(x := w') \). When we decompose the cast, we must make some substitution into \( S_{12} \) and \( S_{22} \), but which? It is clear that we must substitute \( w' \) into \( S_{22} \), since the original application has type \( S_{22}(x := w') \). Decomposing the cast will produce the inner application \( \Delta \vdash w ((S_{21} \Rightarrow S_{11}) \vdash w') : S_{12}(x := (S_{21} \Rightarrow S_{11}) \vdash w') \); in order to apply the codomain cast to this term, we must substitute \( (S_{21} \Rightarrow S_{11}) \vdash w' \) into \( S_{12} \). This calculation determines the form of F_CDECOMP.

While the operational semantics changes only in F_CDECOMP, we have split the evaluation relation into two parts: reductions \( \rightarrow_{h} \) and steps \( \rightarrow_{h} \). This is a technical
change that allows us to factor our proofs more cleanly (particularly for the parallel reduction proofs).

The final change generalizes S_SUB_REFIN to open terms. We must close these terms before we can compare their behavior, using closing substitutions \( \sigma \) and reading \( \Delta \models \sigma \) as “\( \sigma \) satisfies \( \Delta \)”.

Care is needed here to prevent the typing rules from becoming circular: the typing rule S_SUB references the subtyping judgment, the subtyping rule S_SUB_REFIN references the implication judgment, and the single implication rule S_IMP has...
Denotations of types

\[ s \in \llbracket \{ x : B \mid s_0 \} \rrbracket \iff s \rightarrow^* h \land (\exists k \in \mathcal{X}_B. s \rightarrow^* k \land s_0 \{ x := k \} \rightarrow^* \text{true}) \]

\[ s \in \llbracket x : S_1 \rightarrow S_2 \rrbracket \iff \forall q \in \llbracket S_1 \rrbracket. s q \in \llbracket S_2 \{ x := q \} \rrbracket \]

Denotations of kinds

\[ \{ x : B \mid s \} \in \llbracket \bullet \rrbracket \iff \forall k \in \mathcal{X}_B. s \{ x := k \} \in \llbracket \{ x : \text{Bool} \mid \text{true} \} \rrbracket \]

\[ x : S_1 \rightarrow S_2 \in \llbracket \bullet \rrbracket \iff S_1 \in \llbracket \bullet \rrbracket \land \forall q \in \llbracket S_1 \rrbracket. S_2 \{ x := q \} \in \llbracket \bullet \rrbracket \]

Semantic judgments

\[ \Delta \models S_1 < : S_2 \iff \forall \sigma \text{ s.t. } \Delta \models \tau, \llbracket \sigma(S_1) \rrbracket \subseteq \llbracket \sigma(S_2) \rrbracket \]

\[ \Delta \models s : S \iff \forall \sigma \text{ s.t. } \Delta \models \tau, \sigma(s) \in \llbracket \sigma(S) \rrbracket \]

\[ \Delta \models S \iff \forall \sigma \text{ s.t. } \Delta \models \tau, \sigma(S) \in \llbracket \bullet \rrbracket \]

Fig. 8. Type and kind semantics for dependent \( \lambda_H \).

\( \Delta \models \sigma \) in a negative position. This circularity would cause the typing rules to be non-monotonic, and so the existence of the least or the greatest fixed-point would not be immediately obvious—our type system would not be well defined! To avoid this circularity, \( \Delta \models \sigma \) must not refer back to other judgments. (The reader may wonder why this was not a problem in \( \lambda_C \) but notice that in \( \lambda_C \), implication is only used in T.CHECKING—which has no (real) context. If we only needed implication in the S.CHECKING rule, we would not need contexts here, either—we can ensure that active checks only occur at the top-level, with an empty context. But the S.SUB_REFINE subtyping rule refers to S.IMP, and subtyping may be used in arbitrary contexts.)

We can avoid the circularity and ensure that the type system is well defined by building the syntactic rules on top of a denotational semantics for \( \lambda_H \)'s types.\(^4\) The idea is that the semantics of a type is a set of closed terms defined independently of the syntactic typing relation, but that turns out to contain all closed well-typed terms of that type. Thus, in the definition of \( \Delta \models \sigma \), we quantify over a somewhat larger set than strictly necessary—not just the syntactically well-typed terms of appropriate type (which are all the ones that will ever appear in programs) but all semantically well-typed ones.

The type semantics appears in Figure 8. It is defined by induction on type skeletons. For refinement types, terms must either go to blame or produce a constant that satisfies (all instances of) the given predicate. For function types, well-typed arguments must yield well-typed results. By construction, these sets include only terminating terms that do not get stuck. In order to show that casts inhabit the

\(^4\) Knowles and Flanagan (2010) also introduce a type semantics, but their semantics differs from ours in two ways. First, because they cannot treat blame as an exception (because their semantics is nondeterministic), they must restrict the terms in the semantics to be those that only get stuck at failed casts. They do so by requiring the terms to be well typed in the simply typed \( \lambda \)-calculus after all casts have been erased. Secondly, their type semantics does not require strong normalization. However, it is not clear whether their language actually admits nontermination—they include a fix constant, but their semantic type soundness proof appears to break down in that case. The problem is not insurmountable: either step indexing their semantics or a proof of unwinding as in Pitts (2005) would resolve the issue.
denotations of their types, we must also define a denotation of kinds. Since the only kind is $\ast$, its denotation $\llbracket \ast \rrbracket$ directly defines semantic well-formedness in terms of the denotations of types.

We must again make the assumption that constants have most-specific types: if $\llbracket ty_h(k) \rrbracket = B$ and $s \{ x := k \} \rightarrow_h^* \text{true}$ then $\emptyset \vdash ty_h(k) : \{ x : B \mid s \}$. We make some other more standard assumptions as well. Constants must have closed, well-formed types, and the types assigned must be well-formed. We require that constants are semantically well-typed: $k \in \llbracket ty_h(k) \rrbracket$; this requirement is true by our “most-specific type” assumption at base types, but must be assumed at (first-order) function types. Note that this rules out including $\text{fix}$ as a constant, since our type semantics is inhabited only by strongly normalizing terms. We conjecture that expanding the denotation of refinement types to allow for divergence or a step-indexed logical relation (Ahmed 2006) would allow us to consider nonterminating terms.

We introduce a few facts about type semantics before proving semantic type soundness.

4.6 Lemma [Determinacy]: If $s \rightarrow_h s'$ and $s \rightarrow_h s''$, then $s' = s''$.

4.7 Corollary [Coevaluation]: If $s \rightarrow_h^* s'$ and $s \rightarrow_h^* q$, then $s' \rightarrow_h^* q$.

4.8 Lemma [Expansion and contraction of $\llbracket S \rrbracket$]: If $s \rightarrow_h^* s'$, then $s' \in \llbracket S \rrbracket$ iff $s \in \llbracket S \rrbracket$.

Proof
By induction on $|S|$.

4.9 Lemma [Blame inhabits all types]: For all $S$, $\emptyset \vdash l \in \llbracket S \rrbracket$.

Proof
By induction on $|S|$.

4.10 Corollary [Nonemptiness]: For all $S$, there exists some $q$ such that $q \in \llbracket S \rrbracket$.

The normal forms of $\rightarrow_h^*$ are of the form $q = w$ or $\emptyset \vdash l$.

4.11 Lemma [Strong normalization]: If $s \in \llbracket S \rrbracket$, then there exists a $q$ such that $s \rightarrow_h^* q$—i.e., either $s \rightarrow_h^* w$ or $s \rightarrow_h^* \emptyset \vdash l$.

Proof
By induction on $|S|$.

$S = \{ x : B \mid s_0 \}$: Suppose $s \in \llbracket \{ x : B \mid s_0 \} \rrbracket$. By definition, either $s \rightarrow_h^* w$ or $s \rightarrow_h^* \emptyset \vdash l$, so $s$ normalizes.

$S = x : S_1 \rightarrow S_2$: Suppose $s \in \llbracket x : S_1 \rightarrow S_2 \rrbracket$. We know that for any $q \in \llbracket S_1 \rrbracket$ that $s \overset{l}{q} \in \llbracket S_2 \{ x := q \} \rrbracket$. Since $\llbracket S_2 \rrbracket$ is nonempty (by Lemma 4.10), let $q \in \llbracket S_2 \rrbracket$. By the induction hypothesis (IH), $s \overset{l}{q} \rightarrow_h^* w$ or $s \overset{l}{q} \rightarrow_h^* \emptyset \vdash l$. By the definition of evaluation contexts and $\rightarrow_h^*$, the function position is evaluated first. If the application reduces to a value (i.e., $s \overset{l}{q} \rightarrow_h^* w$), then first $s \overset{l}{q} \rightarrow_h^* w$ and so $s \rightarrow_h^* w$. Alternatively, the application could reduce to blame (i.e., $s \overset{l}{q} \rightarrow_h^* \emptyset \vdash l$). There are two ways for this to happen: either $s \rightarrow_h^* \emptyset \vdash l$, or $s \rightarrow_h^* w$ and $q \rightarrow_h^* \emptyset \vdash l$. In both cases $s$ normalizes.
Unlike the rest of the paper, we take a top-down approach to the rest of type soundness to help motivate the steps. We are interested in relating our syntactic type system and the type semantics by semantic type soundness: if $\emptyset \vdash s : S$, then $s \in \llbracket S \rrbracket$. However, to prove this result, we must generalize it. In the bottom of Figure 8, we define three semantic judgments that correspond to each of the three typing judgments. (Note that the third one requires the definition of a kind semantics that picks out well-behaved types—those whose embedded terms belong to the type semantics.) We then show that the typing judgments imply their semantic counterparts.

4.12 Theorem [Semantic-type soundness]:

1. If $\Delta \vdash S_1 <: S_2$ then $\Delta \models S_1 <: S_2$.
2. If $\Delta \vdash s : S$ then $\Delta \models s : S$.
3. If $\Delta \vdash S$ then $\Delta \models S$.

Proof

Proof of (1) is in Lemma 4.14. Proofs of (2) and (3) are in Lemma 4.21.

The first part follows by induction on the subtyping judgment.

4.13 Lemma [Trivial refinements of constants]: If $k \in \mathcal{K}_B$, then $k \in \llbracket \{ x : B \mid \text{true} \} \rrbracket$.

4.14 Lemma [Semantic-subtype soundness]: If $\Delta \vdash S_1 <: S_2$ then $\Delta \models S_1 <: S_2$.

Proof

By induction on the subtyping derivation.

SSUB_REFINE: We know $\Delta \vdash \{ x : B \mid s_1 \} <: \{ x : B \mid s_2 \}$, and must show the corresponding semantic subtyping. Inversion of this derivation gives us $\Delta, x : \{ x : B \mid \text{true} \} \vdash s_1 \Rightarrow s_2$, which means

$$\forall \sigma. ((\Delta, x : \{ x : B \mid \text{true} \} \vdash \sigma \land \sigma(s_1) \rightarrow^*_{\text{true}} \text{true}) \implies \sigma(s_2) \rightarrow^*_{\text{true}} \text{true}) \quad (*)$$

We must show $\Delta \models \{ x : B \mid s_1 \} <: \{ x : B \mid s_2 \}$, i.e., that $\forall \sigma. (\Delta \models \sigma \implies \llbracket \{ x : B \mid s_1 \} \rrbracket \subseteq \llbracket \{ x : B \mid s_2 \} \rrbracket)$. Let $\sigma$ be given such that $\Delta \models \sigma$. Suppose $s \in \llbracket \sigma(\{ x : B \mid s_1 \}) \rrbracket$. By definition, either $s$ goes to $\mathfrak{g}l$, or it goes to $k \in \mathcal{K}_B$ such that $s_1(\{ x := k \} \rightarrow^*_{\text{true}} \text{true}$. In the former case, $\mathfrak{g}l \in \llbracket \{ x : B \mid s_2 \} \rrbracket$ by definition. So consider the latter case, where $s \rightarrow^*_{\text{true}} k$.

We already know that $k \in \mathcal{K}_B$, so it remains to see that $\sigma(s_2)(\{ x := k \} \rightarrow^*_{\text{true}} \text{true}$. We know by assumption that $\sigma(s_1)(\{ x := k \} \rightarrow^*_{\text{true}} \text{true}$. By Lemma 4.13, $k \in \llbracket \{ x : B \mid \text{true} \} \rrbracket$.

Now observe that $\Delta, x : \{ x : B \mid \text{true} \} \vdash \sigma(\{ x := k \}$. Since $\sigma(s_1) \rightarrow^*_{\text{true}} \text{true}$, we can conclude that $\sigma(s_2) \rightarrow^*_{\text{true}} \text{true}$ by our assumption (*). This completes this case.

SSUB_FUN: $\Delta \vdash (x : S_{11} \rightarrow S_{12}) <: (x : S_{21} \rightarrow S_{22})$; by the IH, we have $\Delta \models S_{12} \Rightarrow S_{11}$ and $\Delta, x : S_{21} \models S_{22} \Rightarrow S_{22}$. We must show that $\Delta \models (x : S_{11} \rightarrow S_{12}) <: (x : S_{21} \rightarrow S_{22})$.

Let $\Delta \models \sigma$ and $s \in \llbracket \sigma(x : S_{11} \rightarrow S_{12}) \rrbracket$, for some $\sigma$. We must show, for all $q$, that if $q \in \llbracket \sigma(S_{21}) \rrbracket$ then $s \models q \in \llbracket \sigma(S_{22}) \rrbracket$.

Let $q \in \llbracket \sigma(S_{21}) \rrbracket$. Then $q \in \llbracket \sigma(S_{11}) \rrbracket$. Since $s \in \llbracket \sigma(x : S_{11} \rightarrow S_{12}) \rrbracket$, we know that $s \models q \in \llbracket \sigma(S_{12}) \rrbracket(\{ x := q \} \rrbracket$. Finally, since $\Delta, x : S_{21} \models S_{12} \Rightarrow S_{22}$ and $\Delta, x : S_{21} \models \sigma(\{ x := q \})$, we can conclude that $s \models q \in \llbracket \sigma(S_{22}) \rrbracket(\{ x := q \} \rrbracket$, and so $s \in \llbracket \sigma(x : S_{21} \rightarrow S_{22}) \rrbracket$.  

\[ \square \]
Contracts made manifest

The proof semantic subtype soundness goes through easily, the first of the three parts of semantic soundness (Theorem 4.12). We run into some complications with semantic type and kind soundness, the second and third parts (which must be proven together). The crux of the difficulty lies with the S_APP rule. Suppose the application \( s_1 \ s_2 \) was well typed and \( s_1 \in \llbracket x : S_1 \to S_2 \rrbracket \) and \( s_2 \in \llbracket S_1 \rrbracket \). According to S_APP, the application’s type is \( S_2 \{ x := s_2 \} \). By the type semantics defined in Figure 8, if \( s_1 \in \llbracket x : S_1 \to S_2 \rrbracket \), then \( s_1 \ q \in \llbracket S_2 \{ x := q \} \rrbracket \) for any \( q \in \llbracket S_1 \rrbracket \). Sadly, \( s_2 \) is not necessarily a result! We do know, however, that \( s_2 \in \llbracket S_1 \rrbracket \), so \( s_2 \to^* q_2 \) by strong normalization (Lemma 4.11). We need to ask, then, how the type semantics of \( S_2 \{ x := s_2 \} \) and \( S_2 \{ x := q_2 \} \) relate. (One might think that we can solve this by changing the type semantics to quantify over terms, not results. But this just pushes the problem to the S_LAM case.)

We can show that the two type semantics are in fact equal using a parallel reduction technique. We define a parallel reduction relation \( \Rightarrow \) on terms and types in Figure 9 that allows redexes in different parts of a term (or type) to be reduced in the same step, and we prove that types that parallel-reduce to each other—like \( S_2 \{ x := s_2 \} \) and \( S_2 \{ x := q_2 \} \)—have the same semantics. The definition of parallel reduction is standard, though we need to be careful to make it respect our CBV reduction order: the \( \beta \)-redex \((\lambda x : S_1. \ s_1) \ s_2 \) should not be contracted unless \( s_2 \) is a

\[
\begin{align*}
\text{FP_REFL} & \quad s \Rightarrow s \\
\text{FP_RCONST} & \quad w \Rightarrow w' \\
\text{FP_RCHECK} & \quad \langle \{ x : B \mid s_1 \} \Rightarrow \{ x : B \mid s_2 \} \rangle \Rightarrow k' \\
\text{FP_ROK} & \quad \langle \{ x : B \mid s \} \Rightarrow \{ x : B \mid \text{true}, k \} \rangle \Rightarrow k \\
\text{FP_RFAIL} & \quad \langle \{ x : B \mid s \} \Rightarrow \{ x : B \mid \text{false}, k \} \rangle \Rightarrow \hat{t} \\
\text{FP_RCDECOMP} & \quad (\langle x : S \Rightarrow \text{S_12} \Rightarrow S_21 \Rightarrow S_22 \Rightarrow w_1 \Rightarrow w_1' \Rightarrow w_2 \Rightarrow \text{w_2}' \rangle) \\
\text{FP_LAM} & \quad \lambda x : S_{1}. \ s_{12} \Rightarrow \lambda x : S_{1}' \ s_{12}' \\
\text{FP_APP} & \quad s_{1} \ s_{2} \Rightarrow s_{1}' \ s_{2}' \\
\text{FP_CHECK} & \quad S \Rightarrow S' \\
\text{FP_SREFL} & \quad (x : B \mid s) \Rightarrow (x : B \mid s') \\
\text{FP_SFUN} & \quad x : S_1 \Rightarrow S_2 \Rightarrow x : S_1' \Rightarrow S_2' \\
\text{FP_SREFINE} & \quad S_1 \Rightarrow S_1' \ s_2 \Rightarrow S_2' \\
\end{align*}
\]

Fig. 9. Parallel reduction for dependent \( \lambda_{H} \).
value, since doing so can change the order of effects. (Other redices within $s_1$ and $s_2$
 can safely reduce.)\footnote{We conjecture that the reflexive transitive closure of a similar “CBV-respecting” variant of full $\beta$-
 reduction could be used in place of our parallel reduction. It is not clear whether it would lead to
 shorter proofs.} The proof requires a longish sequence of technical lemmas that
 essentially show that $\Rightarrow$ commutes with $\rightarrow^*_h$. Since the proofs require fussy symbol
 manipulation, we have done these proofs in Coq. Our development is available
 at \url{http://www.cis.upenn.edu/~mgree/papers/lambdah_parred.tgz}. We restate
 the critical results here.

4.15 Lemma [Substitution of parallel-reducing terms, Lemma A3 in thy.v]:
If $w \Rightarrow w'$, then
1. if $s \Rightarrow s'$ then $s\{x := w\} \Rightarrow s'\{x := w'\}$, and
2. if $S \Rightarrow S'$ then $S\{x := w\} \Rightarrow S'\{x := w'\}$.

4.16 Lemma [Parallel reduction implies co-evaluation, Lemma A20 in thy.v]:
If $s_1 \Rightarrow s_2$ then $s_1 \rightarrow^*_h k$ iff $s_2 \rightarrow^*_h k$. Similarly, $s_1 \rightarrow^*_h \upharpoonright l$ iff $s_2 \rightarrow^*_h \upharpoonright l$.

An alternative strategy would be to use $\Rightarrow$ in the typing rules and $\rightarrow^*_h$ in the
 operational semantics. This would simplify some of our metatheory, but it would
 complicate the specification of the language. Using $\rightarrow^*_h$ in the typing rules gives a
 clearer intuition and keeps the core system small.

4.17 Lemma [Single parallel reduction preserves type semantics]:
If $S_1 \Rightarrow S_2$ then $\llbracket S_1 \rrbracket = \llbracket S_2 \rrbracket$.

Proof
By induction on $|S_1|$ (which is equal to $|S_2|$), with a case analysis on the final rule
 used to show $S_1 \Rightarrow S_2$. \hfill \Box

4.18 Corollary [Parallel reduction preserves type semantics]: If $S_1 \Rightarrow^* S_2$ then
$\llbracket S_1 \rrbracket = \llbracket S_2 \rrbracket$.

4.19 Lemma [Partial semantic substitution]: If $\Delta_1, x : S' \vdash s : S$, and $\Delta_1, x : S', \Delta_2 \vdash S$, and $\Delta_1 \vdash s' : S'$ then $\Delta_1, \Delta_2 \{x := s\} \vdash s\{x := s'\} : S\{x := s'\}$ and $\Delta_1, \Delta_2 \{x := s\} \vdash S\{x := s'\}$.

Proof
By the definition of $\Delta \vdash \sigma$. \hfill \Box

The semantic typing case for casts requires a separate induction.

4.20 Lemma [Semantic typing for casts]: If $\Delta \vdash S_1$ and $\Delta \vdash S_2$ and $\llbracket S_1 \rrbracket = \llbracket S_2 \rrbracket$, then $\Delta \vdash \langle S_1 \Rightarrow S_2 \rangle^\top : x : S_1 \rightarrow S_2$ for fresh $x$.

Proof
By induction on $|S_1| = |S_2|$, going by cases on the shape of $S_2$. Let $\Delta \vdash \sigma$; we show
 that $\sigma(\langle S_1 \Rightarrow S_2 \rangle^\top) \in \llbracket \sigma(S_1 \rightarrow S_2) \rrbracket$.\footnotemark
\(S_2 = \{x : B \mid \sigma(s_2)\}\): Let \(q \in \llbracket \sigma(S_1) \rrbracket\). If \(q = \uparrow l'\), then the applied cast goes to \(\uparrow l'\), and we are done by Lemma 4.9. So \(q = k \in \mathcal{X}_B\). By F_CCHECK \(\llbracket S_1 \Rightarrow \{x : B \mid \sigma(s_2)\}\rrbracket l k \rightarrow_h \llbracket\{x : B \mid \sigma(s_2)\}, \sigma(s_2)[x := k], k\rrbracket l\). By the well-kindness of \(S_2\), we know that \(\sigma(s_2)[x := k] \in \llbracket\{x : \text{Bool} \mid \text{true}\}\rrbracket\), so by strong normalization (Lemma 4.11), the predicate in the active check goes to blame or to a value. If it goes to blame, we are done. If it goes to a value, then that value must be true or false. If it goes to false, then the whole term goes to blame and we are done. If it goes to true, then the check will step to \(k\). But \(\sigma(s_2)[x := k] \rightarrow^* \text{true}\), so \(k \in \llbracket \sigma(\{x : B \mid s_2\}) \rrbracket\) by definition. Expansion (Lemma 4.8) completes the proof.

\(S_2 = x : S_2 \rightarrow S_2\): We must have \(S_1 = x : S_1 \rightarrow S_2\). Let \(q \in \llbracket \sigma(S_1) \rrbracket\); if it is blame, we are done by Lemma 4.9, so let it be a value \(w\). Let \(q' \in \llbracket \sigma(S_2) \rrbracket\); if it is blame we are done, so let it be a value \(w'\). By F_CDECOMP:

\[
\llbracket \sigma(S_2)[x := \langle S_2 \Rightarrow S_1 \rangle] w' \rrbracket = \sigma(S_2)[x := w'] (w (\langle S_2 \Rightarrow \sigma(S_1) \rangle w'))
\]

By the IH, \(\langle \sigma(S_2) \Rightarrow \sigma(S_1) \rangle\) is semantically well-typed, so \(\langle \sigma(S_2) \Rightarrow \sigma(S_1) \rangle w' \in \llbracket \sigma(S_1) \rrbracket\). By strong normalization (Lemma 4.11), this term reduces (and therefore parallel reduces, by Lemma 4.4) to some \(q''\).

We know that \(w q'' \in \llbracket \sigma(S_2)[x := q'' \rangle\) by assumption. Using parallel reduction (Corollary 4.18), we have \(\llbracket \sigma(S_2)[x := q'' \rangle = \llbracket \sigma(S_2)[x := \langle \sigma(S_2) \Rightarrow \sigma(S_1) \rangle w' \rangle\rrbracket\rrbracket\).

Before applying the IH, we note that \(\Delta \vdash S_1 \{x := \langle S_2 \Rightarrow S_1 \rangle w' \rangle\) and \(\Delta \vdash S_2 \{x := w' \rangle\) by Lemma 4.19. Then by the IH we see that \(\langle \sigma(S_2)[x := \langle S_2 \Rightarrow S_1 \rangle w' \rangle \Rightarrow \sigma(S_2)[x := w' \rangle \rangle\) is semantically well-kindled, so

\[
\llbracket \sigma(S_1)[x := \langle S_2 \Rightarrow S_1 \rangle w' \rangle \rrbracket = \sigma(S_2)[x := w'] (w w'') \in \llbracket \sigma(S_2) \rrbracket
\]

4.21 Lemma [Semantic-type soundness]:

1. If \(\Delta \vdash s : S\) then \(\Delta \models s : S\).
2. If \(\Delta \vdash S\) then \(\Delta \models S\).

Proof

By induction on the typing and well-formedness derivations, using Corollary 4.18 in the S_APP case and Lemma 4.14 in the S_SUB case.

Theorem 4.12 gives us type soundness, and it combines with Lemma 4.11 for an even stronger result: well-typed programs always evaluate to values of appropriate (semantic) type.

While one can prove progress and preservation theorems, we omit them: we already have type soundness. Our later proofs will require standard weakening and substitution lemmas, though, so we prove them now.

4.22 Lemma [Weakening]: If \(\Delta \vdash s : S\) and \(\Delta \vdash S\), and \(\text{dom}(\Delta) \cap \text{dom}(\Delta') = \emptyset\) with \(\vdash \Delta, \Delta'\), then \(\Delta, \Delta' \vdash s : S\) and \(\Delta, \Delta' \vdash S\).

Proof

By straightforward induction on \(s\) and \(|S|\); we reuse the (critical) context well-formedness derivation in the S_CHECKING case.
The substitution lemma has one complication: The operational judgment $S_{\text{IMP}}$ requires the semantic-type soundness theorem to show that a syntactically well-typed term can be used in a closing substitution. It is otherwise straightforward.

4.23 Lemma [Substitution (implication)]: If $\Delta_1, x : S, \Delta_2 \vdash s_1 \supset s_2$ and $\Delta_1 \vdash s : S$, then $\Delta_1, \Delta_2 \{x := s\} \vdash s_1\{x := s\} \supset s_2\{x := s\}$.

Proof
Direct, unfolding the closing substitutions. □

4.24 Lemma [Substitution (subtyping)]: If $\Delta_1, x : S, \Delta_2 \vdash S_1 <: S_2$ and $\Delta_1 \vdash s : S$, then $\Delta_1, \Delta_2 \{x := s\} \vdash S_1\{x := s\} <: S_2\{x := s\}$.

Proof
By induction on the subtyping derivation. □

4.25 Lemma [Substitution (typing and well-formedness)]: If $\Delta_1 \vdash s : S$ then
1. if $\Delta_1, x : S, \Delta_2 \vdash s_1 : S_1$ then $\Delta_1, \Delta_2 \{x := s\} \vdash s_1\{x := s\} : S_1\{x := s\}$,
2. if $\Delta_1, x : S, \Delta_2 \vdash S_1$ then $\Delta_1, \Delta_2 \{x := s\} \vdash S_1\{x := s\}$, and
3. if $\vdash \Delta_1, x : S, \Delta_2$ then $\vdash \Delta_1, \Delta_2 \{x := s\}$.

Proof
By mutual induction on the typing derivations. □

5 The translations

We divide our treatment of translations between lax $\lambda_C$, $\lambda_H$, and picky $\lambda_C$ into two sections: one for exact translations, moving right on the axis of blame, and another for inexact translations, moving left.

<table>
<thead>
<tr>
<th>Exact translations</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax $\lambda_C$</td>
</tr>
<tr>
<td>$\psi$</td>
</tr>
<tr>
<td>$\phi$</td>
</tr>
<tr>
<td>$\lambda_H$</td>
</tr>
<tr>
<td>picky $\lambda_C$</td>
</tr>
</tbody>
</table>

Inexact translations, more blame in target language

Section 6 covers the exact translations, moving left on the axis of blame from picky $\lambda_C$ to $\lambda_H$, and from $\lambda_H$ to lax $\lambda_C$. Section 7 covers the inexact translations, moving right on the axis of blame from lax $\lambda_C$ to $\lambda_H$, and from $\lambda_H$ to picky $\lambda_C$.

Each translation proof follows the same basic schema. First, we define a logical relation between the two languages. Then we use the logical relation to prove a lemma relating the translation, contracts, and casts. Finally, we prove that the translation preserves evaluation behavior—that is, terms are logically related to their translations—and typing. All of the proofs make extensive use of expansion and
Result correspondence

\[ r \approx q : T \]

Term correspondence

\[ t \sim s : T \]

contraction of evaluation and “cotermination” arguments. Every proof uses its own contract/cast logical relation. The proofs for the inexact translations in Section 7 demand custom term logical relations, too. We have used \( \sigma \) to range over closing substitutions in \( \lambda_H \); we will use \( \delta \) to range over dual closing substitutions in the logical relations.

6 Exact translations

Translations moving left on the axis of blame—from picky \( \lambda_C \) to \( \lambda_H \), and from \( \lambda_H \) to lax \( \lambda_C \)—are exact. That is, we can show a tight behavioral correspondence between terms and their translations (see Figure 10). We read \( t \sim s : T \) as “\( t \) corresponds with \( s \) at type \( T \).”

Our correspondence is a standard logical relation, defined in two intertwined parts: a relation on results, \( r \approx q : T \) and its closure with respect to evaluation, \( t \sim s : T \). The term correspondence is defined directly: terms correspond when they reduce to corresponding results. We write \( \rightarrow_c \) in this single definition: in Section 6.1 we use this definition taking \( \rightarrow_c \) to be \( \rightarrow_{\text{picky}} \); in Section 6.2 we use this definition taking \( \rightarrow_c \) to be \( \rightarrow_{\text{lax}} \). The result correspondence is defined inductively over \( \lambda_C \)’s simple types. Blame corresponds to itself at any type. At \( B \), constants in \( \mathcal{K}_B \) correspond to themselves; results at \( T_1 \to T_2 \) correspond when they applying them to corresponding terms yields corresponding terms. Stratifying the definition this way simplifies some of our proofs later. We call this correspondence exact because terms corresponding at base type yield identical results.

Note that we define the correspondence here on closed (or harmlessly open) terms. In the following two sections, we will define translation specific extensions of the correspondence to open terms and contracts.

6.1 Translating picky \( \lambda_C \) to \( \lambda_H \): dependent \( \phi \)

We define the full \( \phi \) for the dependent calculi in Figure 11. In the dependent case, we need to translate derivations of well-formedness and well-typing of \( \lambda_C \) contexts, terms, and contracts into \( \lambda_H \) contexts, terms, and types. We translate derivations to ensure type preservation, translating \( T_{\text{VAR}}T \) and \( T_{\text{VAR}}C \) derivations differently: we leave variables of simple type alone, but we cast variables bound to contracts.

To see why we need this distinction, consider the function contract \( f : (x : \{ x : \text{Int} \mid \text{pos } x \} \mapsto \{ y : \text{Int} \mid \text{true} \}) \mapsto \{ z : \text{Int} \mid f^0 = 0 \} \). Note that this contract is well formed
in $\lambda_c$, but that the codomain “abuses” the bound variable. A naive translation will not be well typed in $\lambda_h$. The term $f$ will not be typeable when $f$ has type $x : \{x : \texttt{Int} \mid \texttt{pos} x\} \rightarrow \texttt{Int}$, since $f$ only accepts positive arguments. The problem is that SWF.FUN can add a (possibly refined) type to the context when checking the codomain, so we need to restore the “variables have raw types” invariant—something we cannot always rely on subtyping to do, since types are not in general subtypes of their raw type. By tracking the variables that were bound by contracts in $\lambda_c$, we can be sure to cast them to raw types when they are referenced. We therefore translate the contract above to $f : S \rightarrow \{z : \texttt{Int} \mid (\langle S \Rightarrow \texttt{Int} \rightarrow \texttt{Int} \rangle)^f 0 = 0\}$, where $S = x : \{x : \texttt{Int} \mid \texttt{pos} x\} \rightarrow \texttt{Int}$. This (partially) motivates the $x : c^t$ binding form in dependent $\lambda_c$.

Bulletproofing uses raw types, defined here for the dependent system.

\[
\begin{align*}
\{x : B \mid s\} &= \{x : B \mid \texttt{true}\} \\
\{x : S_1 \rightarrow S_2\} &= [S_1] \rightarrow [S_2] \\
\{x : B \mid t\} &= \{x : B \mid \texttt{true}\} \\
\{x : c_1 \mapsto c_2\} &= [c_1] \rightarrow [c_2]
\end{align*}
\]

Note that dependency is eliminated.

We could write the translation on terms instead of derivations, defining

\[
\phi(x : c_1 \mapsto c_2) = x : \phi(c_1) \rightarrow \phi(c_2)\{x := \langle \phi(c_1) \Rightarrow [c_1]t\} x
\]

but the proofs are easier if we translate derivations.

Constants translate to themselves. One technical point: To maintain the raw-type invariant, we need $\lambda_h$’s higher-order constants to have typings that can be seen as raw by the subtyping relation, i.e., $\Delta \vdash t_{y_h}(k) <: [t_{y_c}(k)]$. This can be proven at base types (since we have already assumed that $t_{y_h}(k)$ is the “most specific type” for each $k$), but must be assumed for first-order constant functions. This


\[ c \sim_{l'} S : T \]

\[ \{ x : B \mid t \} \sim_{l'} \{ x : B \mid s \} : B \iff \forall k \in \mathcal{K}_B. \ t \{ x := k \} \sim s \{ x := k \} : \text{Bool} \]

6.1 Lemma [Expansion and contraction]: If \( t \xrightarrow{\text{picky}} t' \), and \( s \xrightarrow{\text{picky}} s' \) then \( t \sim s : T \) iff \( t' \sim s' : T \).

6.2 Lemma [Constants correspond to themselves]: For all \( k, k \sim k : ty_C(k) \).

6.3 Lemma [Equivalence is closed under parallel reduction]: If \( s \Downarrow s' \) then \( t \sim s : T \) iff \( t \sim s' : T \). Similarly, if \( S \Downarrow S' \) then \( c \sim_{l'} S : T \) iff \( c \sim_{l'} S' : T \).

Proof
In both cases, by induction on \( T \), using the first to prove the second. \( \square \)
6.4 Lemma [Trivial casts]: If \( t \sim s : B \) and \( \langle S \rangle = B \), then \( t \sim \langle S \Rightarrow [B] \rangle \).

6.5 Lemma [Related base casts]: If \( \{x : B \mid t\} \sim^{l_0,l_1} \{x : B \mid s\} \) and \( \langle S \rangle = B \), then \( \langle \{x : B \mid t\} \rangle \sim^{l_0,l_1} \langle \{x : B \mid s\} \rangle \).

Proof

Direct. Note that \( l_0 \) and \( l_1 \) are entirely irrelevant.

6.6 Lemma [Bulletproofing]: If \( t \sim s : T \) and \( c \sim^{l''} S \) : \( T \) then \( \langle c \rangle \sim^{l''} \langle S \rangle \).

Proof

By induction on \( T \). First, observe that either both \( t \) and \( s \) go to \( \uparrow l'' \) or both \( t \) and \( s \) go to values related at \( T \). In the former case, the outer terms also go to blame. So we only consider the case where \( t \longrightarrow \uparrow \text{picky}^* v \), \( s \longrightarrow \uparrow h w \), and \( v \approx w : T \).

\[ T = B \]: So \( c = \{x : B \mid t_1\} \) and \( S = \{x : B \mid s_1\} \) and \( S' = \{x : B \mid s_2\} \). By Lemma 6.5 we have \( \langle c \rangle \sim^{l''} \langle S \rangle \). By Lemma 6.4 we can add the extra, trivial cast \( \langle S \Rightarrow \langle S \rangle \rangle \).

\[ T = T_1 \rightarrow T_2 \]: We know that \( c = x : c_1 \rightarrow c_2 \) and \( S = x : S_1 \rightarrow S_2 \). Let \( t' \sim s' : T_1 \). We only need to consider the case where \( t' \longrightarrow \uparrow \text{picky}^* v' \) and \( s' \longrightarrow \uparrow h w' \). Then \( t' \sim \text{picky}^* \uparrow l'' \) and \( s' \longrightarrow \uparrow h \uparrow l'' \) the outer terms correspond because both blame \( l'' \).

On the \( \lambda_C \) side, \( \langle c \rangle \sim^{l''} \langle S \rangle \).

By Lemma 6.5 and \( c_1 \sim^{l''} S_1 : B \), we know that \( \langle c_1 \rangle \sim^{l''} \langle S_1 \rangle \). Both terms go to blame or to the same value—which must be \( k \), from inspection of the contract and cast evaluation rules.. The former case is immediate, since the outer terms then go to blame. So suppose \( \langle c_1 \rangle \sim^{l''} k \longrightarrow \uparrow \text{picky}^* k \) and \( \langle S_1 \rangle \Rightarrow S_1 \rightarrow \uparrow h k \). Now the terms evaluate like so:

\[ \langle c \rangle \sim^{l''} \langle S \rangle \]

\[ \langle S_2 \rangle \sim^{l''} \langle S \rangle \]

By Lemma 6.4, \( k \sim \langle S \rangle \). So \( v \sim \langle S \rangle \). We have by definition (and \( k \sim \langle S \rangle \)) that \( c_2 \{x : c_1 \} \sim^{l''} \langle S \rangle \). Recall that \( \langle S \rangle \Rightarrow S_1 \rightarrow \uparrow h k \). This implies \( \langle S \rangle \Rightarrow S_1 \rightarrow \uparrow h k \) (Lemma A4 in the Coq). We can then see that
6.8 Lemma: If \( t_1 \xrightarrow{\text{picky}} \text{true} \) implies \( t_2 \xrightarrow{\text{picky}} \text{true} \) then \( \emptyset \vdash \phi(\emptyset \vdash t_1 : \text{Bool}) \Rightarrow \phi(\emptyset \vdash t_1 : \text{Bool}) \).

**Proof**

By the logical relation. \( \square \)

The type preservation proof is very similar to the correspondence proof of Theorem 6.7.

---

Having characterized how contracts and pairs of related casts relate, we show that terms correspond to their translation.

**6.7 Theorem [Behavioral correspondence]:** If \( \vdash \Gamma \), then:

1. If \( \phi(\Gamma \vdash t : T) = s \) then \( \Gamma \vdash t \sim s : T \).
2. If \( \phi(\Gamma \vdash l : T) = S \) then \( \Gamma \vdash c \sim l : S : T \).

**Proof**

We simultaneously show both properties by induction on the depth of \( \phi \)'s recursion. \( \square \)

We can now prove that \( \phi \) preserves types, using Theorem 6.7 to show that \( \phi \) preserves the implication judgment. As a preliminary, we use the behavioral correspondence to show that \( \phi \) preserves the implication judgment.

---

By the logical relation. \( \square \)

The type preservation proof is very similar to the correspondence proof of Theorem 6.7.
Term translation

\( \psi : s \to t \)

\[
\begin{align*}
\psi(x) &= x \\
\psi(\lambda x : S. s) &= \lambda x : [S]. \psi(s) \\
\psi((S_1 \Rightarrow S_2)^l) &= (\psi(S_1, S_2))^{l} \\
\psi(\langle x : B | s_1, s_2, k \rangle^l) &= \langle \{x : B | \psi(s_1) \}, \psi(s_2), k \rangle^l
\end{align*}
\]

Cast translation

\( \psi : S \times S \times l \to T \)

\[
\begin{align*}
\psi^l(\{x : B | s_1\}, \{x : B | s_2\}) &= \{x : B | \psi(s_2)\} \\
\psi^l(x : S_{11} \to S_{12}, x : S_{21} \to S_{22}) &= x : \psi^l(S_{21}, S_{11}) \mapsto \psi^l(S_{12} \{x := \langle S_{21} \Rightarrow S_{11} \rangle^l, x\}, S_{22})
\end{align*}
\]

Fig. 13. \( \psi \) mapping dependent \( \lambda_H \) to dependent \( \lambda_C \).

6.9 Theorem [Type preservation]: If \( \phi(\Gamma) = \Delta \) then:

1. \( \Gamma \vdash \Delta \).
2. If \( \phi(\Gamma \vdash t : T) = s \) then \( \Delta \vdash s : [T] \).
3. If \( \phi(\Gamma \vdash l^c, c : T) = S \) then \( \Delta \vdash S \).

Proof

We prove all three properties simultaneously, by induction on the depth of \( \phi \)'s recursion.

The proof is by cases on the \( \lambda_C \) context well-formedness/term typing/contract well-formedness derivations, which determine the branch of \( \phi \) taken. \( \square \)

6.2 Translating \( \lambda_H \) to lax \( \lambda_C \): dependent \( \psi \)

In this section, we formally define \( \psi \) for the dependent versions of lax \( \lambda_C \) and \( \lambda_H \). We prove that \( \psi \) is type preserving and induces behavioral correspondence.

The full definition of \( \psi \) is given in Figure 13. Most terms are translated homomorphically. In abstractions, the annotation is translated by erasing the refined \( \lambda_H \) type to its skeleton. As we mentioned in Section 3, the trickiest part is the translation of casts between function types: when generating the codomain contract from a cast between two function types, we perform the same asymmetric substitution as \( F_{\text{CDecomp}} \). Since \( \psi \) inserts new casts, we need to pick a blame label: \( \psi(\langle S_1 \Rightarrow S_2 \rangle^l) \) passes \( l \) as an index to \( \psi^l(S_1, S_2) \).

We reuse the term correspondence \( t \sim s : T \) (Figure 10), interpreting it as using \( \longrightarrow_{\text{lax}} \), and define a new contract/cast correspondence \( c \sim S_1 \Rightarrow S_2 : T \) (Figure 14), relating contracts and pairs of \( \lambda_H \) types—effectively, casts. This correspondence uses the term correspondence in the base type case and follows the pattern of \( F_{\text{CDecomp}} \) in the function case. Since it inserts a cast in the function case, we index the relation with a label, just like \( \psi \). Note that the correspondence is blame-exact, relating \( \lambda_C \) and \( \lambda_H \) terms that either blame the same label or go to corresponding values. We define closing substitutions ignoring the contracts in the context; we lift the relation to open terms in the standard way.

We begin with some standard properties of the term correspondence relation.
Contract/type correspondence

\[ c \sim S_1 = \downarrow S_2 : T \]

\[ \{ x : B \mid t \} \sim \{ x : B \mid s_1 \} \Rightarrow \{ x : B \mid s_2 \} : B \iff \forall k \in \mathcal{K}_B. t [ x := k ] \sim s_2 [ x := k ] : \text{Bool} \]

\[ x : c_1 \mapsto c_2 \sim x : S_1 \rightarrow{=} S_2 \Rightarrow r \quad \Rightarrow \quad c_1 \sim S_1 \Rightarrow S_1 \rightarrow T_1 \quad \Rightarrow \quad c_1 \sim S_2 \Rightarrow S_2 \rightarrow T_2 \Rightarrow \]

\[ \forall t \sim s : T_1. c_2 [ x := t ] \sim S_1 \{ x := S_1 \rightarrow T_1 \} \Rightarrow S_2 \{ x := S_2 \rightarrow T_2 \} \]

Dual closing substitutions

\[ \Gamma \vDash \delta \iff \begin{cases} \forall x : T \in \Gamma. \delta_1 ( x ) \sim \delta_2 ( x ) : T \\ \forall x : c' \in \Gamma, \delta_1 ( x ) \sim \delta_2 ( x ) : [ c ] \end{cases} \]

Lifted to open terms

\[ \Gamma \vdash t \sim s : T \iff \forall \delta. ( \Gamma \vDash \delta \implies \delta_1 ( t ) \sim \delta_2 ( s ) : T ) \]

6.10 Lemma [Expansion and contraction]: If \( t \rightarrow^{lax^*} t' \), and \( s \rightarrow^* s' \) then \( t \sim s : T \) iff \( t' \sim s' : T \).

6.11 Lemma [Blame corresponds to blame]: For all \( T \), \( \lceil l \sim \lceil l : T \).

6.12 Lemma [Constants correspond to themselves]: For all \( k, k \approx k : ty_c ( k ) \).

As a corollary of Lemmas 6.11 and 6.10, if two terms evaluate to blame, then they correspond. This will be used extensively in the proofs below, as it allows us to eliminate many cases.

6.13 Lemma [Corresponding terms coevaluate]: If \( t \sim s : T \) then \( t \rightarrow^{lax^*} v \land s \rightarrow h v \) or \( t \rightarrow^{lax^*} \lceil l \land s \rightarrow h \lceil l \); moreover, \( t \rightarrow^{lax^*} r \) and \( s \rightarrow^{h} q \) such that \( r \approx q : T \).

6.14 Lemma [Contract/cast correspondence]: If \( c \sim S_1 \Rightarrow S_2 : T \) and \( t \sim s : T \) then \( \langle c \rangle f, l t \sim \langle S_1 \Rightarrow S_2 \rangle f s : T \).

Proof

By induction on \( T \). We reason via expansion (Lemma 6.10), showing that the initial terms reduce to corresponding terms.

\[ T = B : \text{So } c = \{ x : B \mid t_1 \}, S_1 = \{ x : B \mid s_1 \}, \text{ and } S_2 = \{ x : B \mid s_2 \}. \text{ Since } t \sim s : B, \text{ we know that they either both reduce to } k \in \mathcal{K}_B \text{ or } \lceil l \text{. If the latter is the case, we are done. So suppose } t \rightarrow^{lax^*} k \text{ along with } s \rightarrow h k. \]

We can step our terms into active checks as follows:

\[ \{ x : B \mid t_1 \} \rightarrow^{lax^*} \{ x : B \mid s_1 \} \Rightarrow \{ x : B \mid s_2 \} \rightarrow h \{ x : B \mid s_2 \} \}

By inversion of the contract/cast correspondence, we know that \( t_1 [ x := k ] \sim s_2 [ x := k ] : \text{Bool} \), so these terms go to blame or to a \( \text{Bool} \) together. If they go to \( \lceil l \), we are done. If they go to false, then both the obligation and the cast
will go to \( \triangledown l \). Finally, if they both go to true, then both terms will evaluate to \( k \).

\[
T = T_1 \rightarrow T_2 : c = x : c_1 \rightarrow c_2, S_1 = x : S_{11} \rightarrow S_{12}, \text{ and } S_2 = x : S_{21} \rightarrow S_{22}.
\]

We know by inversion of the contract/cast relation that \( c_1 \sim S_{21} \Rightarrow S_{11} : T_1 \) and that for all \( t \sim s : T_1, c_2\{x := t\} \sim S_{12}\{x := \langle S_{21} \Rightarrow S_{11} \rangle^l s\} \Rightarrow S_{22}\{x := s\} : T_2 \). We want to prove that \( \langle c \rangle^l \sim \langle S_1 \Rightarrow S_2 \rangle^l : T_1 \rightarrow T_2 \). First, we can assume \( t \rightarrow_{lax^*} v \) and \( s \rightarrow_h w \) where \( v \sim w : T_1 \rightarrow T_2 \) — if not, both cast and contracted terms go to blame and we are done.

We show that the decomposition of the contract and cast terms correspond for all inputs. Let \( t' \sim s' : T_1 \). Again, we can assume that they reduce to \( v' \sim w' : T_1 \), or else we are done by blame lifting. On the \( \lambda_C \) side, we have

\[
(\langle c \rangle^l t) \rightarrow_{lax^*} \langle c_2\{x := v'\}\rangle^l \langle v \rangle^l \langle c_1 \rangle^l v')
\]

In \( \lambda_H \), we find

\[
(\langle S_1 \Rightarrow S_2 \rangle^l s') \rightarrow_{lax^*} \langle S_{12}\{x := \langle S_{21} \Rightarrow S_{11} \rangle^l w\} \Rightarrow S_{22}\{x := w'\}\rangle^l (w \langle \langle S_{21} \Rightarrow S_{11} \rangle^l w' \rangle)t_2.
\]

By the IH, we know that \( \langle c_1 \rangle^l v' \sim \langle S_{21} \Rightarrow S_{11} \rangle^l w' : T_1 \). Since \( v \sim w : T_1 \rightarrow T_2 \), we have \( v \langle \langle c_1 \rangle^l v' \rangle \sim w \langle \langle S_{21} \Rightarrow S_{11} \rangle^l w' \rangle : T_2 \). Again by the IH, we can see that \( \langle c_2\{x := v'\}\rangle^l \langle v \rangle^l \langle c_1 \rangle^l v') \sim \langle S_{12}\{x := \langle S_{21} \Rightarrow S_{11} \rangle^l w' \} \Rightarrow S_{22}\{x := w'\}\rangle^l w \langle \langle S_{21} \Rightarrow S_{11} \rangle^l w' \rangle : T_2 \). □

We prove three more technical lemmas necessary for the behavioral and type correspondence.

6.15 Lemma [Skeletal equality of subtypes]: If \( \Delta \vdash S_1 <: S_2 \), then \( [S_1] = [S_2] \).

6.16 Lemma: If \( [S_1] = [S_2] = T \), then \( [\psi^l(S_1, S_2)] = T \).

6.17 Lemma: If \( \Delta_1 \vdash S_1 \) and \( \Delta_1 \vdash S_2 \), where \( [S_1] = [S_2] \) then

1. if \( \Delta_1, x : S_1, \Delta_2 \vdash s : S \) then \( \Delta_1, x : S_2, \Delta_2\{x := \langle S_2 \Rightarrow S_1 \rangle^l x\} \vdash s\{x := \langle S_2 \Rightarrow S_1 \rangle^l x\} : S\{x := \langle S_2 \Rightarrow S_1 \rangle^l x\} \), and
2. if \( \Delta_1, x : S_1, \Delta_2 \vdash S \) then \( \Delta_1, x : S_2, \Delta_2\{x := \langle S_2 \Rightarrow S_1 \rangle^l x\} \vdash S\{x := \langle S_2 \Rightarrow S_1 \rangle^l x\} \).

We use the correspondence relations to show that \( s \) and its translation \( \psi(s) \) correspond—i.e., that \( \psi \) faithfully translates the \( \lambda_H \) semantics. We must choose the subject of induction carefully, however, to ensure that we can apply the IH in the case for function casts. An induction on the height of the well-formedness derivation is tricky because of the “extra” substitution that \( \psi \) does. Instead, we do induction on the depth of \( \psi \)’s recursion (and also derivation height, for the \( S_{SUB} \) case).

6.18 Theorem [Behavioral correspondence]:

1. If \( \Delta \vdash s : S \) then \( [\Delta] \vdash \psi (s) \sim s : [S] \).
2. If \( \Delta \vdash S_1 \) and \( \Delta \vdash S_2 \), where \( [S_1] = [S_2] = [S] \), then \( [\Delta] \vdash \psi^l(S_1, S_2) \sim S_1 \Rightarrow^l S_2 : [S] \) (for all \( l \)).
Proof

By induction on the lexicographically ordered pairs \((m,n)\), where \(m\) is the depth of the recursion of the translation \(\psi(s)\) (for part 1) or \(\psi^l(S_1, S_2)\) (for part 2) and \(n\) is either \(|\Delta \vdash s : S|\) (for part 1) or \(|\Delta \vdash S_1| + |\Delta \vdash S_2|\) (for part 2). The first component decreases in all uses of the IH except for the \(S_{\text{SUB}}\) case, where only the second component decreases. Part 1 of the proof proceeds by case analysis on the final rule used in the typing derivation \(\Delta \vdash s : S\). The rule that was used determines the shape of \(\psi(s)\) in all cases but \(S_{\text{SUB}}\).

We give only the most interesting cases for the first part: \(S_{\text{CAST}}, S_{\text{CHECKING}},\) and \(S_{\text{SUB}}\).

1. \(S_{\text{CAST}}:\) \(\Delta \vdash (S_1 \Rightarrow S_2)^l : S_1 \rightarrow S_2\) and \(\psi((S_1 \Rightarrow S_2)^l) = (\psi^l(S_1, S_2))^l\). By inversion, \(\Delta \vdash S_1\) and \(\Delta \vdash S_2\), where \([S_1] = [S_2]\).

   By the IH for proposition (2), \([\Delta] \vdash \psi^l(S_1, S_2) \sim S_1 \Rightarrow^l S_2 : [S_2]\).

   Let \([\Delta] = \delta\); we must show \(\delta_l((\psi^l(S_1, S_2))^l) \sim \delta_2((S_1 \Rightarrow S_2)^l) : [S_1] \rightarrow [S_2]\). Let \(t \sim s : [S_1]\). We have \(\delta_l((\psi^l(S_1, S_2))^l) \sim \delta_2((S_1 \Rightarrow S_2)^l) s : [S_2]\) by Lemma 6.14.

2. \(S_{\text{CHECKING}}:\) We have \(\Delta \vdash \langle \{x:B \mid s_1\}, s_2, k\rangle^l : \{x:B \mid s_1\}\); translating yields \(\psi((\{x:B \mid s_1\}, s_2, k)) = \{x:B \mid \psi(s_1), \psi(s_2), k\}^l\). Recall that the terms of the active check are closed. By inversion we have \(\emptyset \vdash s_2 : \{x:\text{Bool} \mid \text{true}\}\) and \(\emptyset \vdash k : \{x:B \mid \text{true}\}\), so \(k \in \mathcal{K}_B\).

   By the IH, \(\psi(s_2) \sim s_2 : \text{Bool}\). These two terms coevaluate to blame or a boolean constant. There are three cases, all of which result in the active checks evaluating to \(\approx\)-corresponding values:

   - If they go to \(\#l\)’, then the checks do too, and \(\#l’ \approx \#l : B\).
   - If they go to \(\text{false}\), then the checks go to \(\#l\), and \(\#l \approx \#l : B\).
   - If they go to \(\text{true}\), then the checks go to \(k \in \mathcal{K}_B\), and \(k \approx k : B\).

3. \(S_{\text{SUB}}:\) \(\Delta \vdash s : S\); we do not know anything about the shape of \(\psi(s)\). By inversion, \(\Delta \vdash s : S’\) and \(\Delta \vdash S’ < : S\). By Lemma 6.15, \([S’] = [S]\).

   Since the sub-derivation \(\Delta \vdash s : S’\) is smaller, by the IH \([\Delta] \vdash \psi(s) \sim s : [S’]\).

   But \([S’] = [S]\), so we are done.

   Part 2 of this proof proceeds by cases on \(\psi^l(S_1, S_2) = c\).

   \(\psi^l(S_1, \{x:B \mid s_2\}) = \{x:B \mid \psi(s_2)\}\): Note that \(S_2 = \{x:B \mid s_2\}\). By inversion of \(\Delta \vdash \{x:B \mid s_2\}\), we have \(\Delta, x : \{x:B \mid \text{true}\} \vdash s_2 : \{x:\text{Bool} \mid \text{true}\}\).

   By the IH for proposition (1), \([\Delta], x : B \vdash \psi(s_2) \sim s_2 : \text{Bool}\).

   We must show \([\Delta] \vdash \{x:B \mid \psi(s_2)\} \sim S_1 \Rightarrow^l \{x:B \mid s_2\} : B\). Let \([\Delta] = \delta\); we prove that \(\delta_1((\{x:B \mid \psi(s_2)\}) \sim \delta_2((S_1 \Rightarrow S_2)^l) s : [S_2]\) : \(B\), i.e., for all \(k \in \mathcal{K}_B\), that \(\delta_1(\psi(s_2)) x := k \sim \delta_2(s_2) x := k : \text{Bool}\). Since \(k \approx k : B\), we can see this last by the IH.

   \(\psi^l(x : S_{11} \rightarrow S_{12}, x : S_{21} \rightarrow S_{22}) = x : \psi^l(S_{11}, S_{11}) \rightarrow \psi^l(S_{12}, \{x : (S_{21} \Rightarrow S_{11})^l \mid x\}, S_{22})\):

   We can see \(S_2 = x : S_{21} \rightarrow S_{22}\) and so \(S_1 = x : S_{11} \rightarrow S_{12}\), where \([S_2] = [S_{11}]\) and \([S_{22}] = [S_{12}]\). By inversion, we have the following well-formedness derivations:

\[
\Delta \vdash S_{21} \quad \Delta, x : S_{21} \vdash S_{22} \quad \Delta, x : S_{22} \vdash S_{12}
\]
We can apply the IH (contravariantly) to see

\[ [\Delta] \vdash \psi^l(S_{21}, S_{11}) \sim S_{21} \Rightarrow S_{11} : [S_{11}] \quad (*) \]

By weakening (Lemma 4.22), we can see \( \Delta, x : S_{21} \vdash S_{21} \) and \( \Delta, x : S_{21} \vdash S_{11} \). We can reapply the IH to show \( [\Delta], x : [S_{21}] \vdash \psi^l(S_{21}, S_{11}) \sim S_{21} \Rightarrow S_{11} : [S_{11}] \). Now \( \Delta, x : S_{21} \vdash (S_{21} \Rightarrow S_{11})^l : S_{21} \Rightarrow S_{11} \) and \( \Delta, x : S_{21} \vdash (S_{21} \Rightarrow S_{11})^l x : S_{11} \).

By Lemma 6.17, we can substitute this last into \( \Delta, x : S_{11} \vdash S_{12} \{ x := (S_{21} \Rightarrow S_{11})^l x \} \).

We apply the IH for proposition (2) on \( \Delta, x : S_{21} \vdash S_{12}\{ x := (S_{21} \Rightarrow S_{11})^l x \} \) and \( \Delta, x : S_{21} \vdash S_{22} \), showing

\[ [\Delta], x : [S_{21}] \vdash \psi^l(S_{12}\{ x := (S_{21} \Rightarrow S_{11})^l x \}, S_{22}) \sim S_{12}\{ x := (S_{21} \Rightarrow S_{11})^l x \} \Rightarrow S_{22} : [S_{22}] \quad (**) \]

We now combine (*) and (**) to show \( [\Delta] \vdash \psi^l(x : S_{11} \rightarrow S_{12}, x : S_{21} \rightarrow S_{22}) \sim x : S_{11} \rightarrow S_{12} \Rightarrow x : S_{21} \rightarrow S_{22} : [S_{22}] \). Let \( [\Delta] \models \delta \). We can apply (*) to see \( \delta_1(\psi^l(S_{21}, S_{11})) \sim \delta_2(S_{21}) \Rightarrow \delta_2(S_{11}) : [S_{11}] \). For the codomain we must show, for all \( t \sim s : [S_{11}] \), that

\[ \delta_1(\psi^l(S_{12}\{ x := (S_{21} \Rightarrow S_{11})^l x \}, S_{22})) \{ x := t \} \sim \delta_2(S_{12}) \{ x := t \} \Rightarrow \delta_2(S_{22}) \{ x := s \} : [S_{22}] \]

Let \( t \sim s : [S_{11}] \). Recalling that \( [S_{11}] = [S_{21}] \), observe \( [\Delta], x : [S_{21}] \models \delta \{ x := t, s \} \). Call this \( \delta' \). By (**) we see

\[ \delta_1(\psi^l(S_{12}\{ x := (S_{21} \Rightarrow S_{11})^l x \}, S_{22})) \sim \delta_2(S_{12}\{ x := (S_{21} \Rightarrow S_{11})^l x \}) \Rightarrow \delta_2(S_{22}) : [S_{22}] \]

which we can rewrite to

\[ \delta_1(\psi^l(S_{12}\{ x := (S_{21} \Rightarrow S_{11})^l x \}, S_{22})) \{ x := t \} \sim \delta_2(S_{12}) \{ x := t \} \Rightarrow \delta_2(S_{22}) \{ x := s \} : [S_{22}] \]

This is exactly what we needed to finish the proof of correspondence. \( \square \)

As a preliminary to type-preservation, we use behavioral correspondence to show that the implication judgment is preserved.

**6.19 Lemma:** If \( \emptyset \vdash s_1 : \{ x : \text{Bool} \mid \text{true} \} \) and \( \emptyset \vdash s_2 : \{ x : \text{Bool} \mid \text{true} \} \) and \( \emptyset \vdash s_1 \Rightarrow s_2 \), then \( \psi(s_1) \rightarrow_{lax^*} \text{true} \) implies \( \psi(s_2) \rightarrow_{lax^*} \text{true} \).

**Proof**

By the logical relation. \( \square \)

The type preservation proof is very similar to the correspondence proof of Theorem 6.18, though the function case of the type/contract correspondence is intricate.

**6.20 Theorem [Type preservation for \( \psi \)]:**

1. If \( \Delta \vdash s : S \) then \( [\Delta] \vdash \psi(s) : [S] \).
2. If \( \Delta \vdash S_1, \Delta \vdash S_2 \), where \( [S_1] = [S_2] = T \), then \( [\Delta] \vdash \psi^l(S_1, S_2) : T \).
Proof

By induction on the lexicographically ordered pair containing (a) the depth of the recursion of the translation \( \psi \) or \( \psi(s) \), and (b) \( |\Delta \vdash s : S| \) or \( |\Delta \vdash S_1| + |\Delta \vdash S_2| \).

Part 1 of the proof proceeds by case analysis on the final rule of \( \Delta \vdash s : S \), which determines the shape of \( \psi(s) = t \) in all cases but \( S \in \text{UB} \). Part 2 of the proof proceeds by case analysis on \( \psi^l(S_1, S_2) = c \).

\[
\psi^l(x : S_{11} \rightarrow S_{12}, x : S_{21} \rightarrow S_{22}) = x : S^l(S_{21}, S_{11}) \mapsto \psi^l(S_{12})\{x := \langle S_{21} \Rightarrow S_{11}\rangle^l x\}, S_{22}.
\]

We must have \( S_2 = x : S_{21} \rightarrow S_{22} \) and \( S_1 = x : S_{11} \rightarrow S_{12} \), where \([S_{21}] = [S_{11}]\) and \([S_{22}] = [S_{12}]\). By inversion, we have the following well-formedness derivations:

\[
\Delta \vdash S_{21} \quad \Delta \vdash S_{11} \quad \Delta, x : S_{21} \vdash S_{22} \quad \Delta, x : S_{22} \vdash S_{12}
\]

By the IH \( [\Delta] \vdash^l, d \) \( \psi^l(S_{21}, S_{11}) : [S_{11}] \). Note that \([\psi^l(S_{21}, S_{11})] = [S_{21}]\).

By weakening, we can see \( \Delta, x : S_{21} \vdash S_{21} \) and \( \Delta, x : S_{21} \vdash S_{11} \). We can reapply the IH to show \( [\Delta, x : S_{21}] \vdash^{l, d} \psi^l(S_{21}, S_{11}) : [S_{11}] \). Now \( \Delta, x : S_{21} \vdash \langle S_{21} \Rightarrow S_{11}\rangle^l x : S_{11} \). Next \( \Delta, x : S_{21} \vdash \langle S_{21} \Rightarrow S_{11}\rangle^l x : S_{11} \). By Lemma 6.17, we can substitute this last into \( \Delta, x : S_{21} \vdash S_{12} \), finding \( \Delta, x : S_{21} \vdash S_{12}\{x := \langle S_{21} \Rightarrow S_{11}\rangle^l x\} \).

By the IH for proposition (2) on \( \Delta, x : S_{21} \vdash S_{12}\{x := \langle S_{21} \Rightarrow S_{11}\rangle^l x\} \) and \( \Delta, x : S_{21} \vdash S_{22} \),

\[
[\Delta], x : [S_{21}] \vdash^{l, d} \psi^l(S_{12})\{x := \langle S_{21} \Rightarrow S_{11}\rangle^l x\}, S_{22} : [S_{22}]
\]

By Lemma 6.16, \([\psi^l(S_{21}, S_{11})] = [S_{21}]\), so we can rewrite the above derivation to

\[
[\Delta], x : [S_{21}] \vdash^{l, d} \psi^l(S_{12})\{x := \langle S_{21} \Rightarrow S_{11}\rangle^l x\}, S_{22} : [S_{22}]
\]

Now by \text{T\_FUNC}

\[
[\Delta] \vdash^{l, d} x : \psi^l(S_{21}, S_{11}) \mapsto \psi^l(S_{12})\{x := \langle S_{21} \Rightarrow S_{11}\rangle^l x\}, S_{22} : [S_{21}] \rightarrow [S_{22}] \quad \Box
\]

7 Inexact translations

The same translations \( \phi \) and \( \psi \) can be used to move right on the axis of blame (Figure 1). However, in this direction the images of these translations blame strictly more than their pre-images. We were able to use the same correspondence for both exact proofs in Section 6, but the following two proofs use custom correspondences:

one where \( \lambda_C \) terms correspond to \( \lambda_H \) terms (with possibly more blame), and another where \( \lambda_H \) terms correspond to picky \( \lambda_C \) terms (with possibly more blame). In both cases, the \( \lambda_C \) terms will be on the left and the \( \lambda_H \) terms on the right.

7.1 Translating lax \( \lambda_C \) to \( \lambda_H \)

Translating with \( \phi \) from terms in picky \( \lambda_C \) to exactly corresponding terms in \( \lambda_H \) was a relatively straightforward generalization of the non-dependent case; things get more interesting when we consider the translation \( \phi \) from lax \( \lambda_C \) to dependent \( \lambda_H \). We can prove that it preserves types (for terms without active checks), but we can only show a weaker behavioral correspondence: sometimes lax \( \lambda_C \) terms
Value correspondence

\[ v \approx_> w : T \]

\[ k \approx_> k : B \iff k \in \mathcal{K}_B \]

\[ v \approx_> w : T_1 \rightarrow T_2 \iff \forall t \sim_> s : T_1. \ v \ t \sim_> w \ s : T_2 \]

Term correspondence

\[ t \sim_> s : T \iff s \rightarrow^* h \uparrow l \lor (t \rightarrow_{lax}^* v \land s \rightarrow^* w \land v \approx_> w : T) \]

Contract/type correspondence

\[ c \sim_> S : T \iff \forall k \in \mathcal{K}_B. \ t \{x := k\} \sim_> s \{x := k\} : \text{Bool} \]

\[ x : c_1 \mapsto c_2 \sim_> x : S_1 \rightarrow S_2 : T_1 \rightarrow T_2 \iff c_1 \sim_> S_1 : T_1 \land \forall t \sim_> s : T_1. \ c_2 \{x := t\} \sim_> S_2 \{x := s\} : T_2 \]

Dual closing substitutions

\[ \Gamma \vdash \delta \iff \forall x \in \text{dom}(\Gamma). \ \delta_1(x) \sim_> \delta_2(x) : [\Gamma(x)] \]

Lifted to open terms

\[ \Gamma \vdash t \sim_> s : T \iff \forall \delta. \ (\Gamma \vdash \delta \implies \delta_1(t) \sim_> \delta_2(s) : T) \]

\[ \Gamma \vdash c \sim_> S : T \iff \forall \delta. \ (\Gamma \vdash \delta \implies \delta_1(c) \sim_> \delta_2(S) : T) \]

Fig. 15. Blame-inexact correspondence for \( \phi \) from lax \( \lambda \).

terminate with values when their \( \phi \)-images go to blame. This weaker property is a consequence of bulletproofing, the asymmetrically substituting \( F_{CDecomp} \) rule, and the extra casts inserted for type preservation (i.e., for \( T_{VarC} \) derivations). This is not a weakness of our proof technique—we give a counterexample, a lax \( \lambda \) term

\[ \emptyset \vdash t : T \text{ such that } t \rightarrow_{lax}^* v \text{ and } \phi(\emptyset \vdash t : T) \rightarrow^* h \uparrow l. \]

We can show the behavioral correspondence using a blame-inexact logical relation, defined in Figure 15. The behavioral correspondence here, though weaker than before, is still pretty strong: if \( t \sim_> s : B \) (read “\( t \) blames no more than \( s \) at type \( B \)”), then either \( s \rightarrow^* h \uparrow l \) or \( t \) and \( s \) both go to \( k \in \mathcal{K}_B \). This correspondence differs slightly in construction from the earlier exact one—we define \( \approx_> \) as a relation on values, while \( \sim_> \) is a relation on results. Doing so simplifies our inexact treatment of blame—in particular, Lemma 7.2. We again use the term correspondence to relate contracts and \( \lambda_H \) types. We then lift the correspondences to open terms (Figure 15). Closing substitutions map variables to corresponding terms of appropriate type. Note that closing substitutions ignore the contract part of \( x : c[l'] \) bindings, treating them as if they were \( x : [c] \).

7.1 Lemma [Expansion and contraction]: If \( t \rightarrow_{lax}^* t' \), and \( s \rightarrow^* s' \) then \( t \sim_> s : T \) iff \( t' \sim_> s' : T \).

Note that there are corresponding terms at every type. We can prove a much stronger lemma than we did for \( \sim \) in Lemma 6.11, since the correspondence here is much weaker.
7.2 Lemma [Everything corresponds to blame]: For all \( t \) and \( T, t \sim_{>} \hat{t}l : T \).

7.3 Lemma [Constants correspond to themselves]: For all \( k, \ k \approx_{>} k : t\text{y}_c(k) \).

Proof

By induction on \( t\text{y}_c(k) \), recalling that constants are of first order. \( \square \)

As a corollary of Lemmas 7.2 and 7.1, if two terms evaluate to blame—or even just the \( \lambda_H \) side!—then they correspond. This will be used extensively in the proofs below, as it allows us to eliminate many cases.

We prove three lemmas about contracts and casts at base types. The first two characterize contracts and casts at base types.

7.4 Lemma [Trivial casts]: If \( t \sim_{>} s : B \), then \( t \sim_{>} \langle S \Rightarrow [B] \rangle^l : s : B \) for all \( S \).

7.5 Lemma [Related base casts]: If \( \{x : B \mid t\} \sim_{>} \{x : B \mid s\} : B \) and \( t' \sim_{>} s' : B \), then \( \{\{x : B \mid t\}\}^{l''} t' \sim_{>} \langle S \Rightarrow \{x : B \mid s\} \rangle^l : s' : B \) for all \( S \).

The third lemma shows that correspondence is closed under adding extra casts to the \( \lambda_H \) term due to the inexactness of our behavioral correspondence. Since \( \lambda_H \) terms can go to blame more often than corresponding lax \( \lambda_C \) terms, we can add “extra” casts to \( \lambda_H \) terms. We formalize this in the following lemma, which captures the asymmetric treatment of blame by the \( \sim_\succ \) relation. We use it to show that the cast substituted in the codomain by \text{F}_\text{CDECOMP} does not affect behavioral correspondence. Note that the statement of the lemma requires that the types of the cast correspond to some contracts at the same type \( T \), but we never use the contracts in the proof—they witness the well-formedness of the \( \lambda_H \) types.

7.6 Lemma [Extra casts]: If \( t \sim_{>} s : T \) and \( c_1 \sim_{>} S_1 : T \) and \( c_2 \sim_{>} S_2 : T \), then \( t \sim_{>} \langle S_1 \Rightarrow S_2 \rangle^l : s : T \).

Proof

The proof is by induction on \( T \). Note that we do not use \( c_1 \) or \( c_2 \) at all in the proof, but instead they are witnesses to the well-formedness of \( S_1 \) and \( S_2 \).

\[ \lfloor S_1 \rfloor = \lfloor S_2 \rfloor = T. \]

Either \( s \longrightarrow_h^* \hat{t}l' \) or \( t \) and \( s \) both go to corresponding values at \( T \). If \( s \longrightarrow_h^* \hat{t}l' \), then \( \langle S_1 \Rightarrow S_2 \rangle^l s \longrightarrow_h^* \hat{t}l' \) and \( t \sim_{>} \hat{t}l' : T \) since everything is related to blame (Lemma 7.2).

Therefore, suppose that \( t \longrightarrow_{lax}^* v \) and \( s \longrightarrow_h^* w \) and \( v \approx_{>} w : T \) in each of the following cases of induction:

\( T = B \): So \( S_2 = \{x : B \mid s_2\} \), and \( c_2 = \{x : B \mid t_2\} \).

So \( t \longrightarrow_{lax}^* k \) and \( s \longrightarrow_h^* k \) for \( k \in \mathcal{K}_B \). If \( t \) and \( s \) both go to \( k \), then \( \langle S_1 \Rightarrow S_2 \rangle^l s \longrightarrow_h^* \{(x : B \mid s_2), s_2(x := k), k\}^l \).

If \( c_2 \sim_{>} S_2 : B \) we see (in particular) \( t_2\{x := k\} \sim_{>} s_2\{x := k\} : \text{Bool} \).

So \( s_2\{x := k\} \) either goes to \( \hat{t}l' \) or \( s_2\{x := k\} \) (and, irrelevantly, \( t_2\{x := k\} \)) go to some \( k' \in \mathcal{K}_\text{Bool} \).

In the former case, \( \langle \{x : B \mid s_2\}, s_2(x := k), k\rangle^l \longrightarrow_h^* \hat{t}l' \) and we are done (by Lemma 7.2). In the latter case, the \( \lambda_H \) term either goes to \( \hat{t}l \) (and everything is related to blame) or goes to \( k \)—but so does \( t \), and \( k \approx_{>} k : B \).
We have $t \rightarrow^*_{\text{lax}} v$ and $s \rightarrow^*_h w$, where $v \approx > w : T_1 \rightarrow T_2$.

Let $t' \sim > s' : T_1$; we wish to see that $v \sim > (\langle S_1 \Rightarrow S_2 \rangle^l w) s' : T_2$. Either $s' \rightarrow^*_h \emptyset l'$ or both go to values. In the former case the whole cast goes to $\emptyset l'$ we are done by Lemma 7.2, so let $t' \rightarrow^*_{\text{lax}} v'$ and $s' \rightarrow^*_h w'$.

Decomposing the cast in $\lambda_C$,

\[
(\langle S_1 \Rightarrow S_2 \rangle^l w) s' \rightarrow^*_h \\
\langle S_{12}[x := \langle S_{21} \Rightarrow S_{11} \rangle^l w'] \Rightarrow S_{22}[x := w'] \rangle^l (w (\langle S_{21} \Rightarrow S_{11} \rangle^l w'))
\]

We have $c_{21} \sim > S_{21} : T_1$ and $c_{11} \sim > S_{11} : T_1$, so $v' \sim > \langle S_{21} \Rightarrow S_{11} \rangle^l w' : T_1$ by the IH. Since $v \approx > w : T_1 \rightarrow T_2$, we can see that $v v' \sim > w (\langle S_{21} \Rightarrow S_{11} \rangle^l w') : T_2$.

Furthermore, we know that for all $t'' \sim > s'' : T_1$

- $c_{12}[x := t''] \sim > S_{12}[x := s''] : T_2$ and
- $c_{22}[x := t''] \sim > S_{22}[x := s''] : T_2$.

We know that $v' \sim > w' : T_1$ and $v' \sim > \langle S_{21} \Rightarrow S_{11} \rangle^l w' : T_1$, so we can see

- $c_{12}[x := v'] \sim > S_{12}[x := w'] : T_2$ and
- $c_{22}[x := v'] \sim > S_{22}[x := \langle S_{21} \Rightarrow S_{11} \rangle^l w'] : T_2$.

So by the IH,

\[
v v' \sim > \langle S_{12}[x := \langle S_{21} \Rightarrow S_{11} \rangle^l w'] \Rightarrow S_{22}[x := w'] \rangle^l (w (\langle S_{21} \Rightarrow S_{11} \rangle^l w')) : T_2
\]

and we are done by expansion (Lemma 7.1). □

To apply the extra cast lemma, we will need these “witness” contracts for raw types; to that end we define trivial contracts. These contracts are lifted from types, and are the $\lambda_C$ correlate to $\lambda_H$’s raw types.

\[
B \uparrow = \{ x : B \mid \text{true} \} \\
(T_1 \rightarrow T_2) \uparrow = (T_1 \uparrow) \leftrightarrow (T_2 \uparrow)
\]

**7.7 Lemma [Lifted types logically relate to raw types]:** For all $T$, $T \uparrow \sim > [T] : T$.

The “bulletproofing” lemma is the key to the behavioral correspondence proof. We show that a contract application corresponds to bulletproofing with related types. Note that we allow for different types in the two casts. This is necessary due to an asymmetric substitution that occurs when $T = B \rightarrow T_2$.

**7.8 Lemma [Bulletproofing]:** If $t \sim > s : T$ and $c \sim > S : T$ and $c \sim > S' : T$, then $\langle c \rangle^l t \sim > \langle S' \Rightarrow [S'] \rangle^l \langle [S] \Rightarrow S \rangle^l s : T$.

**Proof**

By induction on $T$. First, observe that either $s \rightarrow^*_h \emptyset l''$ or both $t$ and $s$ go to values related at $T$. In the former case, $\langle S' \Rightarrow [S'] \rangle^l \langle [S] \Rightarrow S \rangle^l s \rightarrow^*_h \emptyset l''$, and everything is related to blame (Lemma 7.2). So $t \rightarrow^*_{\text{lax}} v$, $s \rightarrow^*_h w$, and $v \approx > w : T$. 

https://doi.org/10.1017/S0956796812000135 Published online by Cambridge University Press
\(T = B\): So \(c = \{x : B \mid t_1\}\) and \(S = \{x : B \mid s_1\}\) and \(S' = \{x : B \mid s_2\}\). By Lemma 7.5 we have \(\langle c \rangle^{\ell, \ell'} \vdash s : B\). By Lemma 7.4 we can add the extra, trivial cast.

\(T = T_1 \rightarrow T_2\): We know that \(c = x : c_1 \mapsto c_2, S = x : S_1 \rightarrow S_2\) and \(S' = x : S'_1 \rightarrow S'_2\). Let \(t' \vdash s' : T_1\). By Lemma 7.2, we only need to consider the case where \(t' \rightarrow_{\text{tax}} v'\) and \(s' \rightarrow_{\text{h}} w'\) if \(s' \rightarrow_{\text{h}} w''\) we are done. On the \(\hat{\lambda}_C\) side, \(\langle c \rangle^{\ell, \ell'} \vdash (c_2(x := v'))^{\langle \ell, \ell' \rangle} (v ((c_1)^{\ell, \ell'} v'))\). In \(\hat{\lambda}_H\), we can see

\[
\begin{align*}
\langle S' \Rightarrow [S'] \rangle^{\ell} \langle S \Rightarrow S' \rangle^{\ell} s' \rightarrow_{\text{h}}^n & \\
\langle S'_2(x := [S'_1] \Rightarrow S'_1) \rangle^{\ell} w' \Rightarrow [S'_2]^{\ell} (([S'] \Rightarrow S')^{\ell} w) ([S'_1] \Rightarrow S')^{\ell} w' \Rightarrow [S'_2]^{\ell} (w ([S_1] \Rightarrow [S'_1]^{\ell} k))
\end{align*}
\]

By Lemma 7.4, \(k \vdash (S_1 \Rightarrow [S'_1]^{\ell} k) : B\), so \(v k \vdash w ([S_1] \Rightarrow [S'_1]^{\ell} k) : T_2\). Noting that \(k \vdash k : B\) and \(k \vdash (S_1 \Rightarrow [S'_1]^{\ell} k) : B\), we can see that \(c_2\{x := k\} \vdash S_2\{x := k\} : T_2\) and \(c_2\{x := k\} \vdash S'_2\{x := [S'_1] \Rightarrow S'_1\}^{\ell} k) : T_2\). Now the IH shows that \(c_2\{x := k\}^{\langle \ell, \ell' \rangle} (v k) \vdash (S_1 \Rightarrow [S'_1]^{\ell} w') \rightarrow (S'_2) \rightarrow ([S_2] \Rightarrow S_2\{x := k\})^{\ell} (([S_1] \Rightarrow [S'_1]^{\ell} k)) : T_2\), and we conclude the case with expansion (Lemma 7.1).

\(T_1 = T_{11} \rightarrow T_{12}\). We can continue with an application of \(F_{\text{CDECOMP}}\) in \(\hat{\lambda}_H\) and find

\[
\begin{align*}
\langle S'_2(x := [S'_1] \Rightarrow S'_1) \rangle^{\ell} w' \Rightarrow [S'_2]^{\ell} & \\
([S'] \Rightarrow S')^{\ell} w) (([S'_1] \Rightarrow S'_1) \Rightarrow [S'_2]^{\ell} w') \rightarrow_{\text{h}} & \\
\langle S'_2(x := [S'_1] \Rightarrow S'_1) \rangle^{\ell} w' \Rightarrow [S'_2]^{\ell} & \\
([S_2] \Rightarrow S_2\{x := [S'_1] \Rightarrow S'_1\}^{\ell} w') \Rightarrow [S'_2]^{\ell} & \\
(w ([S_1] \Rightarrow [S'_1]^{\ell} \Rightarrow [S'_1]^{\ell} w')) \rightarrow_{\text{h}} &
\end{align*}
\]

By the IH, \(\langle c_1 \rangle^{\ell, \ell'} v' \vdash \langle S_1 \Rightarrow [S'_1]^{\ell} \rangle^{\ell} ([S'_1] \Rightarrow S'_1) \Rightarrow [S'_2]^{\ell} w' : T_1\). By assumption, the results of applying \(v\) and \(w\) to these values correspond. (And they are values, since function contracts/casts applied to values are values.)
We know \( c_1 \sim \succ S'_1 : T_1 \), and by Lemma 7.7 \( T_1 \uparrow \sim \succ [S'_1] : T_1 \). Since \( v' \sim \succ w' : T_1 \), Lemma 7.6 shows \( v' \sim \succ ([S'_1] \Rightarrow [S'_1]) w' : T_2 \). This lets us see that \( c_2 \{ x := v' \} \sim \succ S'_2 \{ x := ([S'_1] \Rightarrow [S'_1]) w' \} : T_2 \) and \( c_2 \{ x := v' \} \sim \succ S_2 \{ x := ([S'_1] \Rightarrow [S'_1]) l \} w' \). Now the IH and expansion (Lemma 7.1) complete the proof. □

Having characterized how contracts and pairs of related casts relate, we show that translated terms correspond to their sources.

7.9 Theorem [Behavioral correspondence]: If \( \Gamma \vdash t : T \), then
1. If \( \phi(\Gamma \vdash t : T) = s \) then \( \Gamma \vdash t \sim \succ s : T \).
2. If \( \phi(\Gamma \vdash l, l' c : T) = s \) then \( \Gamma \vdash c \sim \succ s : T \).

Proof
We simultaneously show both properties by induction on the depth of \( \phi \)'s recursion. To show \( \Gamma \vdash t \sim \succ s : T \), let \( \Gamma \vdash t : \delta \) — we will show \( \delta_1(t) \sim \succ \delta_2(s) : T \).

The proof proceeds by case analysis on the final rule of the translated typing and well-formedness derivations. □

We find a weak corollary: \( \phi(\Gamma \vdash t : B) \rightarrow^* k \) implies \( t \rightarrow^* \lambda_{\text{lax}} k : \) if the \( \lambda_{\text{H}} \) term does not go to blame, then the original \( \lambda_{\text{C}} \) term must go to the same constant.

We can also show type preservation for terms not containing active checks. (We do not know that translated active checks are well typed because Theorem 7.9 is not strong enough to preserve the implication judgment. We only expect these checks to occur at runtime, so this is good enough: \( \phi \) preserves the types of source programs.)

7.10 Theorem [Type preservation]: For programs without active checks, if \( \phi(\vdash \Gamma) = \Delta \), then
1. \( \vdash \Delta \).
2. \( \Delta \vdash \phi(\Gamma \vdash t : T) : [T] \).
3. \( \Delta \vdash \phi(\vdash l, l' c : T) \).

Proof
We prove all three properties simultaneously, by induction on the depth of \( \phi \)'s recursion.

The proof is by cases on the \( \lambda_{\text{C}} \) context well-formedness/term typing/contract well-formedness derivations, which determine the branch of \( \phi \) taken. □

To see that \( \phi \) in Figure 11 does not give us exact blame, let us look at two counterexamples; in both cases, a lax \( \lambda_{\text{C}} \) term goes to a value while its translation goes to blame. In the first example, blame is raised in \( \lambda_{\text{H}} \) due to bulletproofing. In the second, blame is raised due to the extra cast from the translation of \( T_{\text{VarC}} \). In both examples, the contracts are abusive: higher-order contracts where the codomain places a contradictory requirement on the domain. For the first counterexample, let

\[
\begin{align*}
c &= f : (x : \{ x : \text{Int} \mid \text{true} \} \Rightarrow \{ y : \text{Int} \mid \text{nonzero} \ y \} ) \Rightarrow \{ z : \text{Int} \mid f \ 0 = 0 \} \\
S_1 &= x : \{ x : \text{Int} \mid \text{true} \} \Rightarrow \{ y : \text{Int} \mid \text{nonzero} \ y \} \\
S &= \phi(0 \vdash l \ c : (\text{Int} \Rightarrow \text{Int}) \Rightarrow \text{Int}) \\
&= f : S_1 \Rightarrow \{ z : \text{Int} \mid \langle (S_1 \Rightarrow [S_1]) \rangle l \} f \ 0 = 0 \).
\end{align*}
\]
Here, the contradiction comes when the codomain requires that \( f \) yield 0, but \( f' \)'s contract says it will return a non-zero value. We find 
\[
\langle c \rangle \downarrow, l (\lambda f. 0) (\lambda x. 0) \rightarrow^* \gamma l.
\]
For the second counterexample, let 
\[
c' = f : (x : \{ x : \text{Int} \mid \text{nonzero} x \} \rightarrow \{ y : \text{Int} \mid f' 0 = 0 \})
\]
\[
S'_1 = x : \{ x : \text{Int} \mid \text{nonzero} x \} \rightarrow \{ y : \text{Int} \mid \text{true} \}
\]
\[
S' = \phi(0) : (\text{Int} \rightarrow \text{Int}) \rightarrow \text{Int}
\]
\[
f : S'_1 \rightarrow \{ z : \text{Int} \mid (\langle S'_1 \Rightarrow \langle c' \rangle \rangle \downarrow f) 0 = 0 \}.
\]
This time the contradiction comes from the codomain applying \( f \) to 0, while the domain contract requires that \( f' \)'s input be nonzero. We find 
\[
\langle c' \rangle \downarrow, l (\lambda f. 0) (\lambda x. 0) \rightarrow^* \gamma l.
\]
The extra casts that \( \phi \) inserts are all necessary—none can be removed. So while variations on this \( \phi \) are possible, they can only add more casts, which won’t resolve the problem that \( \lambda_H \) blames more.

### 7.2 Translating \( \lambda_H \) to picky \( \lambda_C \)

Terms in \( \lambda_H \) and their \( \psi \)-images in lax \( \lambda_C \) correspond exactly, as shown in Section 6.2. When we change the operational semantics of \( \lambda_C \) to be picky, however, \( \psi(s) \) blames (strictly) more often than \( s \). Nevertheless, we can show an inexact correspondence, as we did for \( \phi \) and lax \( \lambda_C \) in Section 7.1. We use a logical relation \([\sim_\prec]\) for \([\psi]\) into picky \( \lambda_C \) (Figure 16). Here we have reversed the asymmetry: picky \( \lambda_C \) may blame more than \( \lambda_H \). The proof follows the same general pattern: We first show that it is safe to add extra contract checks, then we show that contracts and casts correspond (inexactly), then the correspondence for well-typed terms. We can also show type preservation for source programs (excluding active checks).

**7.11 Lemma [Expansion and contraction]:** If \( t \rightarrow_{\text{picky}}^* t' \) and \( s \rightarrow^*_H s' \) then \( t \prec s : T \iff t' \sim_\prec s' : T \).

**7.12 Lemma [Blame corresponds to everything]:** For all \( T \), \( \gamma l \sim_\prec s : T \).

**7.13 Lemma [Constants correspond to themselves]:** For all \( k, k \approx_\prec k : \text{ty}_c(k) \).

**Proof**

By induction on \( \text{ty}_c(k) \), recalling that constants are of first order. \( \square \)

As a corollary of Lemmas 7.12 and 7.11, if a picky \( \lambda_C \) term evaluates to blame, then it corresponds to any \( \lambda_H \) term. This will be used extensively in the proofs below, as it allows us to eliminate many cases.

**7.14 Lemma [Extra contracts]:** If \( t \prec s : T \) and \( c \prec S_1 \Rightarrow S_2 : T \) then \( \langle c \rangle \downarrow t \prec s : T \).

https://doi.org/10.1017/50956796812000135 Published online by Cambridge University Press
Value correspondence

\[ \forall t. v \approx w : T \\iff \forall k \in \mathcal{K}_B. v \approx k : B \]

\[ \forall t. v \approx w : T \iff \forall t. v \approx w : T \]

Term correspondence

\[ t \approx s : T \iff t \rightarrow \text{picky} \ast \hat{l} \vee t \rightarrow \text{picky} \ast v \land s \rightarrow \ast_\lambda w \land v \approx w : T \]

Contract/type correspondence

\[ \forall c \sim S_1 \Rightarrow S_2 : T \]

\[ \{ x : B \mid t \} \sim \{ x : B \mid s_1 \} \Rightarrow \{ x : B \mid s_2 \} : B \iff \forall k \in \mathcal{K}_B. t \{ x := k \} \sim \{ x := k \} : B \]

Dual closing substitutions

\[ x : c_1 \mapsto c_2 \sim s_1 \rightarrow s_2 \mapsto x : S_1 \rightarrow S_2 = \forall \lambda t_1 \rightarrow t_2 : S_1 \rightarrow S_2 \Rightarrow c_1 \sim S_1 \Rightarrow S_1 \rightarrow S_1 \land \forall \lambda t_1 \rightarrow t_2 : S_1 \rightarrow S_2 \Rightarrow c_1 \sim S_1 \Rightarrow S_1 \rightarrow S_1 \land \forall \lambda t_1 \rightarrow t_2 : S_1 \rightarrow S_2 \Rightarrow c_1 \sim S_1 \Rightarrow S_1 \rightarrow S_1 \]

Lifted to open terms

\[ \Gamma \vdash t \sim s : T \iff \forall \delta. (\Gamma \vdash \delta \implies \delta_1(t) \sim \delta_2(s) : T) \]

\[ \Gamma \vdash c \sim S_1 \Rightarrow S_2 : T \iff \forall \delta. (\Gamma \vdash \delta \implies \delta_1(c) \sim \delta_2(S_1) \Rightarrow \delta_2(S) : T) \]

By definition, applying \( v \) and \( w \) yields related terms at \( T_2 \). Since \( \langle c_1 \rangle^{L,J} v' \sim w' : T_1 \), we have \( c_2 \{ x := \langle c_1 \rangle^{L,J} v' \} \sim S_2 \{ x := \langle S_2 \Rightarrow \}

Proof

By induction on \( T \). If \( t \rightarrow \text{picky} \ast \hat{l}'' \) we are done, so let \( t \rightarrow \text{picky} \ast v \) and \( s \rightarrow \ast_\lambda w \) such that \( v \approx w : T \).

\[ t = B : \text{So } c = \{ x : B \mid t_2 \} \text{ and } S_2 = \{ x : B \mid s_2 \}. \text{ Moreover, } v = w = k \in \mathcal{K}_B, \text{ since those are the only corresponding values at } B. \]

We can step and see \( \langle c \rangle^{L,J} t \rightarrow \text{picky} \ast \langle c, t_2 \{ x := k \} \rangle'. \text{ We know that } t_2 \{ x := k \} \sim \{ x := k \} : \text{Bool}. \text{ There are two possibilities: either } t_2 \{ x := k \} \rightarrow \text{picky} \ast \hat{l}'' \text{ or both terms go to corresponding Bools. In the former case, the whole } \lambda_C \text{ term goes to blame and we are done by Lemma 7.12. If both go to false, then the outer } \lambda_C \text{ term evaluates to } \hat{l} \text{ and we are done by Lemma 7.12 again. If both go to true, then both outer terms go to } k, \text{ and } k \approx k : B. \]

\[ T = T_1 \rightarrow T_2 : \text{So } c = x : c_1 \mapsto c_2 \text{ and } S_1 = x : S_1 \rightarrow S_2 \text{ and } S_2 = x : S_2 \rightarrow S_2. \text{ Let } t' \sim s' : T_1. \text{ If } t' \rightarrow \text{picky} \ast \hat{l}'' \text{ we are done by Lemm 7.12, so let } t' \rightarrow \text{picky} \ast v' \text{ and } s' \rightarrow \ast_\lambda w', \text{ where } v' \approx w' : T_1. \text{ We want to prove } ((\langle c \rangle^{L,J} t) t') \sim s' s' : T_2, \text{ which is true iff:} \]

\[ \langle c_2 \{ x := \langle c_1 \rangle^{L,J} v' \} \rangle^{L,J} (v (\langle c_1 \rangle^{L,J} v')) \sim w w' : T_2 \]

By the IH on \( v \sim w' : T_1 \) and \( c_1 \sim S_2 \Rightarrow S_1 : T_1 \), we have \( \langle c_1 \rangle^{L,J} v' \sim w' : T_1. \text{ By definition, applying } v \text{ and } w \text{ yields related terms at } T_2. \text{ Since } \langle c_1 \rangle^{L,J} v' \sim w' : T_1, \text{ we have } c_2 \{ x := \langle c_1 \rangle^{L,J} v' \} \sim S_2 \{ x := \langle S_2 \Rightarrow \}

https://doi.org/10.1017/509567968120000135 Published online by Cambridge University Press
7.15 Lemma [Contract/cast correspondence]: If \( c \sim s \Rightarrow T \) and \( t \sim s \Rightarrow T \) then \( \langle c \rangle^{l,d} t \sim \langle s \Rightarrow T \rangle^{r} s \Rightarrow T \).

**Proof**

By induction on \( T \). We reason via expansion (Lemma 7.11), showing that the initial terms reduce to corresponding terms.

\( T = B \) : So \( c = \{ x : B \mid t_1 \} \), \( S_1 = \{ x : B \mid s_1 \} \), and \( S_2 = \{ x : B \mid s_2 \} \). Since \( t \sim s \Rightarrow B \), we know that they either both reduce to \( k \in \mathcal{H}_B \) or \( t \longrightarrow_{\text{picky}}^* k' \).

If the latter is the case, we are done. So suppose \( t \longrightarrow_{\text{picky}}^* k \) along with \( s \longrightarrow_{h}^* k \).

We can step our terms into active checks as follows:

\[
\langle \{ x : B \mid t_1 \} \rangle^{l,d} t \longrightarrow_{\text{picky}}^* \langle \{ x : B \mid t_1 \} \rangle^{k} k \]

\[
\langle \{ x : B \mid s_2 \} \rangle^{l,d} s \longrightarrow_{h}^* \langle \{ x : B \mid s_2 \} \rangle^{k} k
\]

By the contract/cast correspondence, we know that \( t_1 \{ x \equiv k \} \sim s_2 \{ x \equiv k \} : \text{Bool} \), so either \( t_1 \{ x \equiv k \} \) goes to blame or both terms go to a \text{Bool} together. In the former case, the outer \( \lambda_c \) term goes to blame and we are done by Lemma 7.12. If they go to false, then both the active check goes to \( \#l \) and we are done, again by Lemma 7.12. Finally, if they both go to true, then both terms will evaluate to \( k \in \mathcal{H}_B \), and \( k \sim k : B \).

\( T = T_1 \rightarrow T_2 \) : \( c = x : c_1 \rightarrow c_2 \), \( S_1 = x : s_{11} \rightarrow s_{12} \), and \( S_2 = x : s_{21} \rightarrow s_{22} \). We know by inversion of the contract/cast relation that \( c_1 \sim S_2 \Rightarrow S_{11} : T_1 \) and that for all \( l'' \) and \( s \sim s : T_1 \), \( c_2 \{ x \equiv t \} \sim S_{12} \{ x \equiv S_{21} \Rightarrow S_{11} \Rightarrow T_1 \} \Rightarrow S_{22} \{ x \equiv s \} : T_2 \). We want to prove that \( \langle c \rangle^{l,d} \sim \langle s \Rightarrow T_1 \rangle^{r} s : T_1 \rightarrow T_2 \).

First, we can assume \( t \longrightarrow_{\text{picky}}^* v \) and \( s \longrightarrow_{h}^* w \), where \( v \sim w : T_1 \rightarrow T_2 \) if not, both the contracted terms go to blame and we are done by Lemma 7.12. We show that the decomposition of the contract and cast terms correspond for all inputs. Let \( t' \sim s' : T_1 \). Again, we can assume that they reduce to \( v' \sim w' : T_1 \), or else we are done by blame lifting in \( \lambda_c \). On the \( \lambda_c \) side, we have

\[
\langle (c) \rangle^{l',d} t' \longrightarrow_{\text{picky}}^* \langle c_2 \{ x \equiv (c_1)^{l',d} v' \} \rangle^{l,d} (v ((c_1)^{l,d} v'))
\]

In \( \lambda_{II} \), we find

\[
\langle S_{12} \{ x \equiv S_{21} \Rightarrow S_{11} \Rightarrow w \} \rangle^{r} w \Rightarrow S_{22} \{ x \equiv w' \} \rangle^{r} (w ((S_{21} \Rightarrow S_{11} \Rightarrow w'))
\]

By the IH, we know that \( \langle c_1 \rangle^{l,d} v' \sim (S_{21} \Rightarrow S_{11})^{r} w' : T_1 \). Since \( v \sim w : T_1 \rightarrow T_2 \), we have \( v' ((c_1)^{l,d} v') \sim w ((S_{21} \Rightarrow S_{11})^{r} w') : T_2 \). By Lemma 7.14, \( \langle c_1 \rangle^{l,d} v' \sim w' : T_1 \). We can then see that \( c_2 \{ x \equiv (c_1)^{l,d} v' \} \sim S_{12} \{ x \equiv (S_{21} \Rightarrow S_{11})^{r} w' \} \Rightarrow S_{22} \{ x \equiv w' \} : T_2 \). By the IH, we therefore have

\[
\langle c_2 \{ x \equiv (c_1)^{l,d} v' \} \rangle^{l,d} (v ((c_1)^{l,d} v')) \sim
\]

\[
\langle S_{12} \{ x \equiv (S_{21} \Rightarrow S_{11})^{r} w' \} \rangle^{r} w \Rightarrow S_{22} \{ x \equiv w' \} \rangle^{r} (w ((S_{21} \Rightarrow S_{11} \Rightarrow w')) : T_2 \)
\]
7.16 Theorem [Behavioral correspondence]:

1. If $\Delta \vdash s : S$ then $[\Delta] \vdash \psi(s) \sim_s s : [S]$.  
2. If $\Delta \vdash S_1$ and $\Delta \vdash S_2$, where $[S_1] = [S_2] = [S]$, then $[\Delta] \vdash \psi^l(S_1, S_2) \sim_s S_1 \Rightarrow S_2 : [S]$.

Proof

By an induction similar to the proof of Theorem 6.18. □

7.17 Theorem [Type preservation for $\psi$]: For programs without active checks, if $\vdash \Delta$, then:

1. If $\Delta \vdash s : S$ then $[\Delta] \vdash \psi(s) : [S]$.  
2. If $\Delta \vdash S_1$, $\Delta \vdash S_2$, where $[S_1] = [S_2] = T$, then $[\Delta] \vdash^{lid} \psi^l(S_1, S_2) : T$.

Proof

By an induction similar to the proof of Theorem 6.20. □

Here is an example where a $\lambda_H$ term reduces to a value while its $\psi$-image in picky $\lambda_C$ term reduces to blame. As before, this counterexample uses an abusive contract: a higher-order contract where the codomain puts a contradictory requirement on the domain. Here, the contradiction is that $f$ claims to return a nonzero value, but the codomain requires that it returns 0.

$$S_1 = f : S_{11} \to S_{12}$$

$$S_2 = f : S_{21} \to S_{22}$$

Let $w = (\langle f : x : \text{Int} | \text{true} \rangle \to \langle y : \text{Int} | \text{nonzero} y \rangle). 0$ and $w' = (\lambda x : \langle x : \text{Int} | \text{true} \rangle. 0). 0$. The term is well-typed: we can show $\emptyset \vdash w : S_1$ and $\emptyset \vdash w' : S_{21}$. Therefore, $\emptyset \vdash (S_1 \Rightarrow S_2)^l (w) \Rightarrow^*_\emptyset 0$. Translating, we find

$$\psi((S_1 \Rightarrow S_2)^l w) \Rightarrow^*_\emptyset 0,$$

On the one hand, $((S_1 \Rightarrow S_2)^l w) \Rightarrow^*_\emptyset 0$, while $((c)^l \lambda f : \text{Int}. 0) \Rightarrow^*_\emptyset \emptyset l$. This means we cannot hope to use $\psi$ as an exact correspondence between $\lambda_H$ and picky $\lambda_C$. (Removing the extra cast $\psi$ inserts into $S_{12}$ does not affect our example, since $\psi$ ignores $S_{12}$ here.) For example,

$$\psi^l([z : \text{Int} | \text{true}] f : \langle S_{21} \Rightarrow S_{11} \rangle^l f, \{z : \text{Int} | f 0 = 0\}) = \{x : B | \psi(f 0 = 0)\}.$$

7.3 Alternative calculi

There are three alternative calculi that we have not considered here: indy $\lambda_C$ (Dimoukas et al. 2011), superpicky $\lambda_H$, and nonterminating calculi. We describe them in detail below, but we leave them as future work.
Dimoulas et al. (2011) add a third blame label to $\lambda_C$, representing the contract itself; we write it here as a subscript. They accordingly change the picky E.CDECOMP rule:

$$\langle x : c_1 \mapsto c_2 \rangle_{l'}^{id} v_1 \rightarrow_{ind} \langle c_2 \{ x := \langle c_1 \rangle_{l'}^l v_2 \} \rangle_{l'}^{id} (v_1 (\langle c_1 \rangle_{l'}^l v_2))$$

In the substitution in the codomain, note that the blame label on the domain contract uses the contract’s blame label $l''$. The intuition here is that any problem arising in $c_2$ is in the contract’s context (label $l''$), not the original negative context (label $l'$). We conjecture (but have not proven) that indy $\lambda_C$ is in the same position on the axis of blame as picky $\lambda_C$. We only need to change the labels on the contracts $\phi$ inserts to have an exact correspondence; however, $\psi$ will remain inexact.

Superpicky $\lambda_H$ reworks the F.CDECOMP rule in an attempt to harmonize $\lambda_H$ and picky $\lambda_C$ semantics:

$$\langle x : S_{11} \rightarrow S_{12} \Rightarrow x : S_{21} \rightarrow S_{22} \rangle_{l}^l w_1 \rightarrow_h \langle S_{12} \{ x := S_{21} \Rightarrow S_{11} \rangle_{l}^l w_2 \Rightarrow S_{22} \{ x := S_{11} \Rightarrow S_{21} \rangle_{l}^l (\langle S_{21} \Rightarrow S_{11} \rangle_{l}^l w_2) \rangle_{l}^l (w_1 (\langle S_{21} \Rightarrow S_{11} \rangle_{l}^l w_2))$$

This seems to resolve the problem with $\psi$ into picky $\lambda_C$, but it poses problems in the proof of semantic-type soundness for $\lambda_H$: how do $S_{22} \{ x := w_2 \}$ and $S_{22} \{ x := S_{11} \Rightarrow S_{21} \rangle_{l}^l (\langle S_{21} \Rightarrow S_{11} \rangle_{l}^l w_2)$ relate?

Finally, we have been careful to ensure that all of our calculi are strongly normalizing. We do not believe this to be essential, though we would have to change our logical relations—$\lambda_H$’s type semantics and the correspondences—to account for nontermination. We conjecture that step-indexing (Ahmed 2006) will suffice.

8 Related work

Conferences in recent years have seen a profusion of papers on higher-order contracts and related features. This is all to the good, but for newcomers to the area it can be a bit overwhelming, especially given the great variety of technical approaches. To help reduce the level of confusion, in Table 1 we summarize the important points of comparison between a number of systems that are closely related to ours. This table is an updated version compared to that in Greenberg et al. (2010).

The largest difference is between latent and manifest treatments of contracts—i.e., whether contract checking (under whatever name) is a completely dynamic matter or whether it leaves a “trace” that the type system can track.

Another major distinction (labeled “dep” in the figure) is the presence of dependent contracts or, in manifest systems, dependent function types. Latent systems with dependent contracts also vary in whether their semantics is lax or picky.

Next, most contract calculi use a standard CBV order of evaluation (“eval order” in the figure). Notable exceptions include those of Hinze et al. (2006), which is embedded in Haskell, Flanagan (2006), which uses a variant of call-by-name, and Knowles and Flanagan (2010), which uses full $\beta$-reduction (more on this below).

---

6 This idea is due to Jeremy Siek (personal communication, January 2010).
Table 1. Comparison between contract systems

<table>
<thead>
<tr>
<th>Latent systems</th>
<th>FF02</th>
<th>HJL06</th>
<th>GF07 $\lambda_C$</th>
<th>BM06</th>
<th>DFFF11</th>
<th>our $\lambda_C$</th>
</tr>
</thead>
<tbody>
<tr>
<td>dep (6)</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>(7)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>eval order</td>
<td>CBV</td>
<td>lazy</td>
<td>CBV</td>
<td>CBV</td>
<td>CBV</td>
<td>CBV</td>
</tr>
<tr>
<td>blame (8)</td>
<td>$\uparrow l$</td>
<td>$\uparrow l$</td>
<td>$\uparrow l$</td>
<td>$\uparrow l$ or $\perp$</td>
<td>$\uparrow l$</td>
<td>$\uparrow l$</td>
</tr>
<tr>
<td>checking (9)</td>
<td>if</td>
<td>if</td>
<td>active</td>
<td>active</td>
<td>active</td>
<td>active</td>
</tr>
<tr>
<td>typing (10)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>n/a</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>any con (11)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Manifest systems</th>
<th>GF07 $\lambda_H$</th>
<th>F06 (12)</th>
<th>KF10 (13)</th>
<th>WF09 (14)</th>
<th>OTMW04 (15)</th>
<th>BGIP11 (16)</th>
</tr>
</thead>
<tbody>
<tr>
<td>dep (6)</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>eval order</td>
<td>CBV</td>
<td>CBN(17)</td>
<td>CBV</td>
<td>CBV</td>
<td>CBV</td>
<td>CBV</td>
</tr>
<tr>
<td>blame (8)</td>
<td>$\uparrow l$</td>
<td>stuck</td>
<td>$\uparrow l$</td>
<td>full $\beta$</td>
<td>$\uparrow l$</td>
<td>$\uparrow l$</td>
</tr>
<tr>
<td>checking (9)</td>
<td>✓</td>
<td>✓</td>
<td>active</td>
<td>active</td>
<td>if</td>
<td>active</td>
</tr>
<tr>
<td>typing (10)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>any con (11)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
</tr>
</tbody>
</table>

Notes: (1) Findler & Felleisen (2002). (2) Hinze et al. (2006). (3) Gronski & Flanagan (2007). (4) Blume & McAllester (2006). (5) Dimoulas et al. (2011). (12) Flanagan (2006). (13) Knowles & Flanagan (2010). (14) Wadler & Findler (2009). (15) Ou et al. (2004). (6) Does the system include dependent contracts or function types (√) or not (×) and, for latent systems, is the semantics lax or picky? (see text for more on “indy” checking). (7) An “unusual” form of dependency, where negative blame in the codomain results in nontermination. (17) A nondeterministic variant of CBN. (8) Do failed contracts raise labeled blame ($\uparrow l$), raise blame without a label ($\uparrow$), get stuck, or sometimes raise blame and sometimes diverge ($\perp$)? (9) Is contract or cast checking performed using an “active check” syntactic form (active), an “if” construct with a refined typing rule (if), or “inlined” by making the operational semantics refer to its own reflexive and transitive closure (○)? (10) Is the typing relation monotonic, i.e., is the typing relation known to be uniquely defined? (11) Are arbitrary user-defined boolean functions allowed as contracts or refinements (√), or only built-in ones (×)?

Another point of variation (“blame” in the figure) is how contract violations or cast failures are reported—by raising an exception or by getting stuck. We also return to this below.

The next two rows in the table (“checking” and “typing”) concern more technical points in the papers most closely related to ours. In both Flanagan (2006) and Gronski and Flanagan (2007), the operational semantics checks casts “all in one go”:

$$s_2\{x := k\} \rightarrow^*_{h} \text{true}$$

$$\langle\{x:B | s_1\} \Rightarrow \{x:B | s_2\}\rangle^l_{h} k \rightarrow_{h} k$$
Such rules are formally awkward, and in any case they violate the spirit of a small-step semantics. Also, the formal definitions of $\lambda_H$ in both Flanagan (2006) and Gronski and Flanagan (2007) involve a circularity between the typing, subtyping, and implication relations. Knowles and Flanagan (2010) improve the technical presentation of $\lambda_H$ in both respects. In particular, they avoid circularity (as we do) by introducing a denotational interpretation of types and maintain small-step evaluation by using a new syntactic form of “partially evaluated casts” (like most of the other systems).

The main contributions of the present paper are (1) the dependent translations $\phi$ and $\psi$ and their properties, and (2) the formulation and metatheory of dependent $\lambda_H$. (Dependent $\lambda_C$ is not a contribution on its own: many similar systems have been studied, and in any case its properties are simple.) The non-dependent part of our $\phi$ translation essentially coincides with the one studied by Gronski and Flanagan (2007), and our behavioral correspondence theorem is essentially the same as their theorem. Our $\psi$ translation completes their story for the non-dependent case, establishing a tight connection between the systems. The full dependent forms of $\phi$ and $\psi$ studied here are novel, as is the observation that the correspondence between the latent and manifest worlds is more problematic in this setting.

Our formulation of $\lambda_H$ is most comparable to that of Knowles and Flanagan (2010), but there are some significant differences. First, our cast-checking constructs are equipped with labels, and failed casts go to explicit blame—i.e., they raise labeled exceptions. In the $\lambda_H$ of Knowles and Flanagan (2010) (though not the earlier one of Gronski and Flanagan (2007)), failed casts are simply stuck terms—their progress theorem says, “If a well-typed term cannot step, then either it is a value or it contains a stuck cast.” Second, their operational semantics uses full, nondeterministic $\beta$-reduction, rather than specifying a particular order of reduction, as we have done. This significantly simplifies parts of the metatheory by allowing them to avoid introducing parallel reduction. We prefer standard CBV reduction because we consider blame as an exception—a computational effect—and we want to reason about which blame will be raised by expressions involving many casts. At first glance, it might seem that our theorems follow directly from the results for Knowles and Flanagan’s language (2007), since CBV is a restriction of full $\beta$-reduction. However, the reduction relation is used in the type system (in rule S_IMP), so the type systems for the two languages are not the same. For example, suppose the term $\text{bad}$ contains a cast that fails. In our system $\{y:B \mid \text{true}\}$ is not a subtype of $\{y:B \mid (\lambda x:S. \text{true}) \text{bad}\}$ because the contract evaluates to blame. However, the subtyping does hold in the Knowles and Flanagan system (2007) because the predicate reduces to true.

The system studied by Ou et al. (2004) is also close in spirit to our $\lambda_H$. The main difference is that, because their system includes general recursion, they restrict the terms that can appear in contracts to just applications involving predefined constants: only “pure” terms can be substituted into types, and these do not include lambda-abstractions. Our system (like all of the others in Table 7—see the row labeled “any con”) allows arbitrary user-defined boolean functions to be used as contracts.
Our description of $\lambda_C$ is ultimately based on $\lambda_{\text{Con}}$ (Findler & Felleisen 2002), though our presentation is slightly different in its use of checks. Hinze et al. (2006) adapted Findler and Felleisen-style contracts (2002) to a location-passing implementation in Haskell, using picky-dependent function contracts.

Our $\lambda_H$-type semantics in Section 4.2 is effectively a semantics of contracts. Blume and McAllester (2006) offer a semantics of contracts that is slightly different—our semantics includes blame at every type, while theirs explicitly excludes it. Xu et al. (2009) is also similar, though their “contracts” have no dynamic semantics at all: they are simply specifications.

Dimoulas et al. (2011) introduce a new dialect of picky $\lambda_C$, where contract checks in the codomain are given a distinct negative label. If labels represent “contexts” for values, then this treats the contract as an independent context. “Indy” $\lambda_C$ and picky $\lambda_C$ will raise exactly the same amount of blame, but they will blame different labels.

Belo et al. (2011) at once simplify and extend the CBV $\lambda_H$ given here. The type system is redesigned to avoid subtyping and closing substitutions, so type soundness is proved with easy syntactic methods (Wright & Felleisen 1994). The language also allows general refinements—refinements of any type, not just base types—and extends the type system to polymorphism. This can be seen as completing some of the future work of Greenberg et al. (2010).

We have discussed only a small sample of many papers on contracts and related ideas. We refer the reader to Knowles and Flanagan (2010) for a more comprehensive survey. Another useful resource is Wadler and Findler (2007) (technically superceded by Wadler and Findler (2007), but with a longer related work section), which surveys work combining contracts with type Dynamic and related features.

There are also many other systems that employ various kinds of precise types, but in a completely static manner. One notable example is the work of Xu et al. (2009), which uses user-defined boolean predicates to classify values (justifying their use of the term “contracts”) but checks statically that these predicates hold.

Sage (Knowles et al. 2006) and Knowles and Flanagan (2010) both support mixed static and dynamic checking of contracts, using, for example, a theorem prover. We have not addressed this aspect of their work, since we have chosen to work directly with the core calculus $\lambda_H$, which for them was the target of an elaboration function.

9 Conclusion

We can faithfully encode dependent $\lambda_H$ into $\lambda_C$—the behavioral correspondence is tight. $\lambda_H$’s F.CDECOMP rule forces us to accept a weaker behavioral correspondence when encoding $\lambda_C$ into $\lambda_H$, so we conclude that the manifest and latent approaches are not equivalent in the dependent case. We do find, however, that the two approaches are entirely inter-encodable in the non-dependent restriction.

Acknowledgments

Sewell and Zappa Nardelli’s OTT tool (Sewell et al., 2007) was invaluable for organizing our definitions. We used Aydemir and Weirich’s LNGen tool (June...
2010) for the Coq development of parallel reduction. Brian Aydemir, João Belo, Chris Casinghino, Nate Foster, and the anonymous POPL reviewers gave us helpful comments. The anonymous JFP reviewers’ thorough comments significantly improved and clarified the paper. Our work has been supported by the National Science Foundation under grants 0702545 (A Practical Dependently-Typed Functional Programming Language), 0910786 (TRELLYS), 0534592 (Linguistic Foundations for XML View Update), and 0915671 (Contracts for Precise Types).

References


