Contracts Made Manifest

Michael Greenberg  
*University of Pennsylvania*

Benjamin C. Pierce  
*University of Pennsylvania, bcpierce@cis.upenn.edu*

Stephanie Weirich  
*University of Pennsylvania, sweirich@cis.upenn.edu*

Follow this and additional works at: [http://repository.upenn.edu/cis_papers](http://repository.upenn.edu/cis_papers)

Part of the [Computer Sciences Commons](http://repository.upenn.edu/cis_papers)

Recommended Citation


Michael Greenberg, Benjamin Pierce, and Stephanie Weirich. **Contracts Made Manifest.** In 37th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages (POPL), pages 353-364, Madrid, Spain, January 2010. ACM  
© ACM, 2010. This is the author's version of the work. It is posted here by permission of ACM for your personal use. Not for redistribution. The definitive version was published in ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages, ([01/2010]) [http://doi.acm.org/10.1145/1706299.1706341](http://doi.acm.org/10.1145/1706299.1706341)* Email permissions@acm.org  
doi:10.1145/1706299.1706341

This paper is posted at ScholarlyCommons. [http://repository.upenn.edu/cis_papers/630](http://repository.upenn.edu/cis_papers/630)  
For more information, please contact libraryrepository@pobox.upenn.edu.
Contracts Made Manifest

Abstract
Since Findler and Felleisen introduced higher-order contracts, many variants have been proposed. Broadly, these fall into two groups: some follow Findler and Felleisen 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, who defined a latent calculus lambdac and a manifest calculus lambdah, gave a translation phi from lambdac to lambdah, and proved that, if a lambdac term reduces to a constant, then so does its phiimage. We enrich their account with a translation psi from lambdah to lambdac 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 lambdah and two dialects (“lax” and “picky”) of lambdac, establish type soundness-a substantial result in itself, for lambdah-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.

Disciplines
Computer Sciences

Comments

© ACM, 2010. This is the author's version of the work. It is posted here by permission of ACM for your personal use. Not for redistribution. The definitive version was published in ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages, (01/2010) http://doi.acm.org/10.1145/1706299.1706341 Email permissions@acm.org
doi:10.1145/1706299.1706341

This conference paper is available at ScholarlyCommons: http://repository.upenn.edu/cis_papers/630
Contracts Made Manifest

Michael Greenberg  
University of Pennsylvania  
Philadelphia, PA

Benjamin C. Pierce  
University of Pennsylvania  
Philadelphia, PA

Stephanie Weirich  
University of Pennsylvania  
Philadelphia, PA

Abstract

Since Findler and Felleisen [2002] introduced higher-order contracts, many variants have been proposed. Broadly, these fall into two groups: some follow Findler and Felleisen 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; others use extended translations preserve behavior in one direction but, in the other, sometimes yield terms that blame more.

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 $\lambda_l$ and two dialects (“lax” and “picky”) of $\lambda_c$, establish type soundness—a substantial result in itself, for $\lambda_l$—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.

Categories and Subject Descriptors  D.3.1 [Programming Languages]: Formal Definitions and Theory—Semantics  ; D.2.4 [Software Engineering]: Software/Program Verification—Programming by contract

General Terms Languages, Theory

Keywords Contract, refinement type, dynamic checking, blame, precondition, postcondition, translation

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 \{x:int | pos x\} $\rightarrow$ 1, 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 \{x:int | pos x\} $\rightarrow$ 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

\{x:int | nonzero x\} $\rightarrow$ \{x:int | pos x\} $\rightarrow$ $\lambda x$.int. pred x

“wraps” the function $\lambda x$.int. pred x 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 pos x, raising $\uparrow l$ if this fails (e.g., if the wrapped function is applied to 1).

Findler and Felleisen’s work sparked a resurgence of interest in contracts, and in the intervening years a bewildering variety of related systems have 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, Hinze et al. [2006], Blume and McAllester [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 2006] are a well-known example in this style; others include the work of Ou et al. [2004], Walder and Findler [2009], and Gronski et al. [2006].

The key feature of manifest systems is that descriptions like \{x:int | nonzero x\} are incorporated into the type system as refinement types. Values of refinement type are introduced via casts like \{x:int | true\} $\rightarrow$ \{x:int | nonzero x\}$\uparrow n$, which has static type \{x:int | nonzero x\} and $\uparrow n$ 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:

\begin{align} f &= (I \rightarrow I \Rightarrow P \rightarrow \hat{o}_l \rightarrow \lambda x.\hat{i}.\ b) x, \end{align}

where $I$ = \{x:int | true\} and $P$ = \{x:int | pos x\}. The sequence of events when $f$ is applied to some argument $n$ (of type $P$) is similar to what we saw before: first, $n$ is cast from $P$ to $I$ (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 $I$ to $P$, raising $\uparrow l$ if this fails.

One point to note here is that casts have just one label, while contract checks in the latent system have two. This difference is not fundamental, but rather a question of the pragmatics of assigning responsibility: both latent and manifest systems can be given more or less rich algebras of blame. Informally, a function contract check
\(\langle c_1 \mapsto c_2 \rangle^{H}\) 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 doesn’t pass \(c_1\), I refuse responsibility (\(\checkmark\))", whereas if \(f\)’s result for good arguments doesn’t satisfy \(c_2\), I accept responsibility (\(\checkmark\)).” In a manifest system, the programmer who writes \(\langle R_1 \mapsto R_2 \Rightarrow S_1 \rightarrow S_2 \rangle^H\) 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 OK 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 \(\checkmark\) 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 seem intuitively to be much the same thing as typecasts in manifest systems, the formal correspondence is not immediate. This has 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 is intuitively a homomorphism: 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 final result \(k\), then so does its translation \(\phi(t)\).

Our work extends theirs in two directions. First, we strengthen their main result by introducing a new homomorphic 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 \(\phi\).) This shows that the manifest and latent approaches are effectively equivalent in the nondependent 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 checked when the bound variable appears the codomain contract? This leads to two dialects of \(\lambda_C\), one which does recheck (picky \(\lambda_C\) and one which does not (lax \(\lambda_C\)). The choice is not clear—dependent contract systems have typically used the lax rule, while the picky one is arguably more correct—so we consider both. In \(\lambda_H\), 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 the definitions, plus an intricate sequence of technical lemmas involving parallel reduction to establish type soundness. (Although Gronski and Flanagan worked only with nondependent \(\lambda_C\) and \(\lambda_H\), Knowles and Flanagan [2009] showed soundness for a variant of dependent \(\lambda_H\) in which order of evaluation is nondeterministic and failed casts get stuck instead of raising blame. See Section 7.)

Surprisingly, the tight correspondence between \(\lambda_C\) and \(\lambda_H\) breaks down in the dependent case: the natural generalization of the translations does not preserve blame exactly. Indeed, we can place \(\lambda_H\) between the two variants of \(\lambda_C\) on an “axis of blame” (Figure 1), where behavior is preserved exactly when moving left on the axis (from picky \(\lambda_C\) to \(\lambda_H\) to lax \(\lambda_C\)), but translated terms can blame more than their pre-images when moving right. The discrepancy arises in the case of “abusive” contracts, such as:

\[f : (N \mapsto I) \mapsto \{z : \text{Int} \mid f = 0\},\]

where \(I = \{x : \text{Int} \mid \text{true}\}\) and \(N = \{x : \text{Int} \mid \text{ nonzero}\ x\}\). 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 \(\lambda_C\)) to \(\lambda_f : \text{Int} \mapsto \text{Int}\) 0 and then apply the result to \(\lambda_x : \text{Int} \times x\) and 5, the final result will be 5, since \(\lambda_x : \text{Int} x\) does satisfy the contract \(\{x : \text{Int} \mid \text{ non zero}\ x\} \mapsto \{y : \text{Int} \mid \text{true}\}\) and 5 satisfies the contract \(\{x : \text{Int} \mid (\lambda_x : \text{Int} x) = 0\} = 0\). However, the translation of \(f\) into \(\lambda_H\) inserts an extra check, wrapping the occurrence of \(f\) in the codomain contract with a cast from \(N \mapsto I\) to \(I \mapsto I\), which fails when the wrapped function is applied to 0. We discuss this phenomenon in greater detail in Section 4.

In summary, our main contributions are (a) the translation \(\psi\) and a symmetric version of Gronski and Flanagan’s behavioral correspondence theorem, (b) the basic metatheory of (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.

A long version of the paper with definitions and proofs in full can be found at http://www.cis.upenn.edu/~mgree/papers/contracts_tr.pdf.

2. The nondependent languages

We begin in this section by defining the nondependent 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, 5, and 6. Throughout the paper, rules prefixed with an \(E\) or a \(F\) 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 \(\lambda_H\).

The language \(\lambda_C\)

The language \(\lambda_C\) is the simply typed lambda calculus straightforwardly augmented with contracts. The most interesting feature is the contract term \(\langle c \rangle^{H,t}\), which, when applied to a term \(t\), dynamically ensures that \(t\) and its surrounding context satisfy \(c\). If \(t\) doesn’t satisfy \(c\), then the positive label \(t\) will be blamed and the whole term will reduce to \(\bot\); on the other hand, if the context doesn’t treat \(\langle c \rangle^{H,t}\) as \(c\) demands, then the negative label \(\not\!t\) will be blamed and the term will reduce to \(\bot\). Contracts come in two forms: base contracts \(\{x : B \mid t\}\) over a base type \(B\) and higher-
from constants to constants (or blame, to allow for partiality). Denotations must agree with \( \text{ty}_c \). We assume that \( B \) is among the base types, with \( \mathcal{K}_{\text{Bool}} = \{ \text{true, false} \} \).

The operational semantics is given in Figure 4. It includes six rules for basic (small-step, call-by-value) 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. As usual, values (and results) do not stop.

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 first-order, we know that when \( \text{E\_CONST} \) applies to a well-typed application, the argument is not just a value, but a constant.

The rules \( \text{E\_CCHECK}, \text{E\_OK}, \text{E\_FAIL} \) and \( \text{E\_CDECOMP} \) describe the semantics of contracts. In \( \text{E\_CCHECK} \), 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. If the check evaluates to true, then \( \text{E\_OK} \) returns the initial constant. If false, the check has failed and a contract has been violated, so \( \text{E\_FAIL} \) steps the term to \( \uparrow l \). Higher-order contracts on a value \( v \) wait to be applied to an additional argument. When that argument has also been reduced to a value \( v' \), \( \text{E\_CDECOMP} \) decomposes the function cast: the argument value is checked with the argument part of the contract (switching positive and negative blame, since the context
Types
\[ S ::= \{ x:B \mid s_1 \} \mid S_1 \rightarrow S_2 \]

Terms, values, results, and evaluation contexts
\[ s ::= x \mid k \mid \lambda x:S_1 \mid s_2 \mid s_1 s_2 \mid \uparrow l \mid \langle \{ x:B \mid s_1 \}, s_2, k \rangle \]
\[ w ::= k \mid \lambda x:S_1 \mid s_2 \mid \langle \{ x:B \mid s_1 \}, s_2, k \rangle \mid \langle S_1 \rightarrow S_2 \Rightarrow S_2 \rangle \mid w \]
\[ q ::= w \mid \uparrow l \]
\[ F ::= [] s \mid w [] \mid \{ \{ x:B \mid s_1 \}, [], k \} \]

Figure 6. Syntax for \( \lambda H \)

is responsible for the argument), and the result of the application is checked with the result contract.

The typing rules for \( \lambda C \) (Figure 5) are mostly standard. We give types to constants using the type-assignment function \( \tau_C \). Blame expressions have all types. Contracts are checked for well-formedness using the judgment \( \vdash c : T \), comprising the rules T_BASEC, which requires that the checking term in a base contract return a boolean value when supplied with a term of the right type, and T_FUN/C. Note that the predicate \( t \) in a contract \( \{ x:B \mid t \} \) can contain at most \( x \) free, since we are considering only nondependent 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 \( k \), that the check expression \( t_2 \) has a boolean type, and that the check is actually checking the right contract. The latter condition is formalized by the T_IMP rule: \( t_2 \Rightarrow t_1 \{ x := k \} \) assures 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 \( \{ x:Int \mid \text{pos}\ x \}, \text{true}, 0 \} \) should not be well typed; and second, we use this property in showing that the translations are type preserving (see Section 5). This rule obviously makes typechecking for the full “internal language” with checks undecidable, but excluding checks recovers decidability.

The language \( \lambda H \)

Our second core calculus, nondependent \( \lambda H \), extends the simply typed lambda-calculus with refinement types and cast expressions. The syntax appears in Figure 6. 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. 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 \( \{ S_1 \Rightarrow S_2 \} \) 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 \( \llbracket \cdot \rrbracket \). Type assignment is via \( \tau_H \), which we assume conforms well-formed types. To keep the languages in sync, we require that \( \tau_H \) and \( \tau_C \) agree on “type skeletons”: if \( \tau_H(k) = B_1 \rightarrow B_2 \), then \( \tau_C(k) = \{ x:B_1 \mid s_1 \} \rightarrow \{ x:B_2 \mid s_2 \} \).

The small-step, call-by-value semantics in Figure 7 comprises six basic rules and two rules involving evaluation contexts \( F \). Each rule corresponds closely to its counterpart in \( \lambda C \).

Notice how the decomposition rules compare. In \( \lambda C \), the term \((c_1 \iff c_2) \rightarrow v\ w\) 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 \((\{ S_1 \Rightarrow S_2 \} \rightarrow \{ S_2 \Rightarrow S_2 \}) \wedge (w \Rightarrow (\{ S_2 \Rightarrow S_3 \} \wedge (v \wedge (\{ S_2 \Rightarrow S_3 \} \wedge w')) \Rightarrow \{ S_2 \Rightarrow S_3 \}) \) does not decompose further, but the behavior is a bit more subtle. The contravariant check \( \{ S_2 \Rightarrow S_3 \} \wedge w' \) makes \( w' \) a suitable input for \( w \), while \( \{ S_2 \Rightarrow S_3 \} \wedge w' \) checks the result from \( w \) applied to (the cast) \( w' \).

Figure 7. Operational semantics for \( \lambda H \)

We define a similar operator, \( \llbracket \cdot \rrbracket : S \rightarrow T \) (pronounced “erase \( S \)”),

\[ \{ x:B \mid s_1 \} \Rightarrow B \]
\[ \llbracket S_1 \Rightarrow S_2 \rrbracket = \llbracket S_1 \rrbracket \Rightarrow \llbracket S_2 \rrbracket \]

These operations apply to \( \lambda C \) contracts and types in the natural way. Type well-formedness 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_CHECKING plays a role analogous to the T_CHECKING rule in \( \lambda C \), using the operational S_IMP rule to guarantee that we only have sensible terms in the predicate position.

An important difference is that \( \lambda H \) has subtyping. The S_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 sub-
type’s condition evaluates to true. For function types, we use the
standard contravariant subtyping rule. We do not consider source
programs with subtyping, since this makes type checking undecid-
able\(^2\); subtyping is just a technical device for ensuring type preser-

between static and dynamic checking that allow for decidable type systems
and subtyping.

<table>
<thead>
<tr>
<th>Δ ⊢ s : S</th>
<th>x : S ∈ Δ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Δ ⊢ x : S</td>
<td>Δ ⊢ k : ty(_h)(k)</td>
</tr>
<tr>
<td>Δ ⊢ S(_1) \xrightarrow{S} S(_2)</td>
<td>Δ \xrightarrow{λx : S(_1), s(_2) : S(_1) → S(_2)}</td>
</tr>
<tr>
<td>Δ ⊢ s(_1) \xrightarrow{s(_2) : S(_2)}</td>
<td>Δ \xrightarrow{S(_1) \xrightarrow{s(_2) : S(_2)}}</td>
</tr>
<tr>
<td>Δ ⊢ S</td>
<td>Δ \xrightarrow{\emptyset : S}</td>
</tr>
<tr>
<td>Δ ⊢ s : S(_1) \xrightarrow{s(_2) : S(_2)}</td>
<td>Δ \xrightarrow{s : S(_1) \xrightarrow{s(_2) : S(_2)}}</td>
</tr>
</tbody>
</table>

\(|\{x : \text{Int} \mid \text{true}\} \implies \{y : \text{Int} \mid \text{pos} \ y\}\)\(^{l,t}\) translates to\(\{\{x : \text{Int} \mid \text{nonzero} \ x\} \implies \{\text{Int} \implies \{y : \text{Int} \mid \text{pos} \ y\}\}\)\(^{l,t}\)

Translating from \(λc\) to \(λt\), we are moving from a simple type
system to a rich one. The translation \(ϕ\) (essentially the same as
Gronski and Flanagan’s) generates terms in \(λt\) with raw types—\(λt\)
types with trivial refinements, corresponding to \(λc\)’s simple types.

Whereas the difficulty with \(ψ\) is ensuring that the checks match
up, the difficulty with \(ϕ\) is ensuring that the terms in \(λc\) and \(λt\) will
blame the same labels. We deal with this problem by translating
a single contract with two blame labels into two separate casts.

The operation of casting into and out of raw types is a kind of
“buletproofing.” Bulletproofing maintains the raw-type invariant:
the positive cast takes \(x\) out of \([c]\) and the negative cast returns it
there. For example,
\(|\{x : \text{Int} \mid \text{nonzero} \ x\} \implies \{y : \text{Int} \mid \text{pos} \ y\}\)\(^{l,t}\)
translates to the $\lambda_1$ term

$$\lambda : [\text{Int} \rightarrow \text{Int}].$$

$$\langle \{x \in \text{Int} \mid \text{nonzero } x \} \Rightarrow ([\text{Int} \rightarrow \text{Int}])^l', \{x \in \text{Int} \mid \text{nonzero } x \} \Rightarrow \{y \in \text{Int} \mid \text{pos } y\}^l \rangle \ f.$$  

The domain of the negative cast checks that $f$’s argument is nonzero with $\{[\text{Int}] \Rightarrow \{x \in \text{Int} \mid \text{nonzero } x\}\}^l$. The domain of the positive cast does nothing, since $\{([\text{Int}] \Rightarrow \{x \in \text{Int} \mid \text{nonzero } x\}) \Rightarrow [\text{Int}]\}^l$ 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 $\lambda_1$ to keep track of blame labels, mimicking $\lambda_c$. This embodies the idea of contracts as pairs of projections [Findler 2006]. Note that ballotproofing is “overkill” at base type: for example, $\langle [\text{Int}] \mid \text{nonzero } x \rangle \to \{y \in \text{Int} \mid \text{pos } y\}^l \ f$.

4. The dependent languages

We now extend $\lambda_c$ to dependent function contracts and $\lambda_1$ to dependent functions. The changes are summarized in Figure 9 (for $\lambda_c$) and Figures 10 and 11 (for $\lambda_1$). Very little needs to be changed in $\lambda_c$, since contracts and types barely interact; the changes to $\text{E}_1\text{CDECOMP}$ and $\text{T}_\text{FUNC}$ are the important ones. Adding dependency to $\lambda_1$ is more involved. In particular, adding contexts to the subtyping judgment entails adding contexts to $\text{S}_\text{IMP}$. To avoid a dangerous circularity, we define closing substitutions in terms of a separate type semantics. Additionally, the new $\text{F}_1\text{CDECOMP}$ rule has a slightly tricky (but necessary) asymmetry, explained below.

**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 Chiti 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.

The new $\text{T}_\text{REPLACE}$, $\text{T}_\text{FUNC}$, and $\text{E}_1\text{CDECOMP}$ rules in Figure 9 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, tracking the labels on a contract check throughout the contract well-formedness judgment. Note that $\text{T}_\text{FUNC}$ adds $x : c_1 \to c'$ to the context when checking the codomain of a function contract, swapping blame labels. We add a new variable rule, $\text{T}_\text{VARC}$, that treats $x : c \to c'$ as if it were its skeleton, $x : c$. While unnecessary for $\lambda_c$, this new binding form helps $\phi$ preserve types. (See Section 6.1).

Two different variants of the $\text{E}_1\text{CDECOMP}$ rule can be found in the literature: we call them 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 $c'$ into $c_2$, Hinze et al. [2006] choose instead to be picky, substituting $(c_1 \to c_2)$'s argument is nonzero before making its 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 $\text{E}_1\text{CDECOMP}$ in Sections 5.1 and 6.2, and lax $\lambda_c$ using only $\text{E}_1\text{CDECOMP}$ in Sections 5.2 and 6.1.

**Dependent $\lambda_1$**

Now we come to the challenging part: dependent $\lambda_1$ and its proof of type soundness.3 These results require the most complex metatheory in the paper, because we need some strong properties about call-by-value evaluation. (The benefit of a CBV semantics is a better treatment of blame. By contrast, Knowles and Flanagan [2009] cannot treat failed casts as exceptions because that would destroy confluence. They treat them as stuck terms.) The needed extensions are detailed in Figures 10 and 11.4

---

3 The proof of type soundness for this system is significantly different from the soundness proof in Knowles and Flanagan [2009], where the operational semantics of $\lambda_1$ is full, nondeterministic $\beta$-reduction. At first glance, it might seem that our theorems follow directly from the results for Knowles and Flanagan’s language, since CBV is a restriction of full $\beta$-reduction. However, the reduction relation is used in the type system (in rule $\text{S}_\text{IMP}$), 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 $\{y : \text{Int} \mid \text{true}\}$ is not a subtype of $\{x : \text{Int} \mid \langle \lambda x : \text{S}_\text{true} \mid \text{true}\rangle\}$ because the contract evaluates to blame. However, the subtyping does hold in the Knowles and Flanagan system because the predicate reduces to true.

4 The semantics in these figures is the same as that of Knowles and Flanagan [2009] except for the evaluation relation, the treatment of blame, and a change to the type semantics that we discuss below.
Types

\[ S ::= \{ x : B \mid s \} \mid x : S_1 \rightarrow S_2 \]

Operational semantics

\[
\begin{align*}
((x : S_1 \rightarrow S_2 \Rightarrow x : S_2) \mapsto x : S_2) w' \mapsto_1 \\
(S_1 x := (S_2 \mapsto S_1) w') \Rightarrow S_2 \{ x := w' \}'
\end{align*}
\]

\[ F_{C\text{DECOMP}} \]

Typing rules

\[
\begin{align*}
\Delta \vdash s_1 : (x : S_1 \rightarrow S_2) & \quad \Delta \vdash s_2 : S_1 \\
\Delta, x : \{ x : B \mid \text{true} \} & \vdash s : \{ x : \text{Bool} \mid \text{true} \}
\end{align*}
\]

\[ \text{SWF}_{\text{REFINE}} \]

\[
\begin{align*}
\Delta \vdash S_1 \quad \Delta, x : S_1 \vdash S_2 & \quad \Delta \vdash S_1 \rightarrow S_2 \\
\Delta, x : \{ x : B \mid \text{true} \} & \vdash s_1 \supset s_2
\end{align*}
\]

\[ \text{SWF}_{\text{FUN}} \]

\[
\begin{align*}
\Delta \vdash S_1 < S_1 & \quad \Delta, x : S_2 \vdash S_2 < S_2 & \quad \Delta \vdash S_1 \rightarrow S_2 < S_2
\end{align*}
\]

\[ \text{SSUB}_{\text{REFINE}} \]

\[
\begin{align*}
\forall \sigma. (\Delta \vdash \sigma \land \sigma(s_1) \mapsto^* \sigma(s_2) \rightarrow \text{true}) & \implies \sigma(s_2) \mapsto^* \sigma(s_1) \rightarrow \text{true} \\
\Delta \vdash s_1 \supset s_2
\end{align*}
\]

\[ \text{S}_{\text{IMP}} \]

Closing substitutions

\[
\begin{align*}
\emptyset \vdash \emptyset \\
\Delta \{ x := s \} \vdash \sigma(x := s)
\end{align*}
\]

\[ \text{SCS}_{\text{EMPTY}} \]

Denotations of types and kinds

\[
\begin{align*}
s \in \{ x : B \mid s \} \iff s \mapsto^* \lambda l & \quad \lor (k \in \text{Kind}, s \mapsto^* k \land s_0(x := k) \mapsto^* \text{true}) \\
s \in \{ x : S_1 \rightarrow S_2 \} & \iff \forall q \in \{ S_1 \}, s q \in \{ S_2(x := q) \} \\
\{ x : B \mid s \} \in \{ * \} & \iff \forall k \in \text{Kind}. \\
x : S_1 \rightarrow S_2 \in \{ * \} & \iff S_1 \in \{ * \} \quad \land \quad \forall q \in \{ S_1 \}, S_2(x := q) \in \{ * \}
\end{align*}
\]

Semantic judgments

\[
\begin{align*}
\Delta \vdash S_1 < S_2 & \iff \forall \sigma. \text{s.t. } \Delta \vdash \sigma \quad \land (\sigma(S_1) \subseteq \sigma(S_2)) \\
\Delta \vdash S & \iff \sigma(S) \in \{ * \}
\end{align*}
\]

Figure 11. Type and kind semantics for dependent \( \lambda t \)

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

Care is needed here to prevent the typing rules from becoming circular: the typing rule \( S_{\text{SUB}} \) references the subtyping judgment, the subtyping rule \( S_{\text{SUB}_{\text{REFINE}}} \) references the implication judgment, and the single implication rule \( \text{S}_{\text{IMP}} \) has \( \Delta \vdash \sigma \) in a negative position. To avoid circularity, \( \Delta \vdash \sigma \) must not refer back to the other judgments.

We can achieve this by building the syntactic rules on top of a denotational semantics for \( \lambda t \)’s types. The idea is that the semantics of a type is a set of closed terms that is 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 \( \Delta \vdash \sigma \), 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 11. 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 go to well-typed results. By construction, these sets include only terminating terms that do not get stuck.

4.1 Lemma [Strong normalization]: If \( s \in \{ S \} \), then there exists a \( q \) such that \( s \mapsto^* q \) i.e., either \( s \mapsto^* w \) or \( s \mapsto^* \lambda l \).

The main things we want to know about the type semantics is semantic type soundness: if \( \emptyset \vdash s : S \), then \( s \in \{ S \} \). However, to prove this, we must generalize it. In the bottom of Figure 11, 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.

\[^5\text{Knowles and Flanagan [2009] also introduce a type semantics, but it differs from ours in two ways. First, because they cannot treat blame as an exception (because their semantics is nondeterministic) they must restrict the terms in the semantics to be those that only get stuck at failed casts. They do so by requiring the terms to be well-typed in the simply typed lambda calculus after all casts have been erased. Secondly, their type semantics does not require strong normalization. However, it is not clear whether their language actually admits nontermination—they include a fix constant, but their type semantics soundness proof appears to break down in that case.}\]
Result correspondence

\[
k \approx k : B \iff k \in \mathcal{K}_B
\]
\[
v \approx w : T_1 \rightarrow T_2 \iff \forall t \sim s : T_1, v t \sim w s : T_2
\]
\[
\top l \approx \top l : T
\]

Term correspondence

\[
t \sim s : T \iff t \rightarrow^* r \land s \rightarrow^* h q \land r \approx q : T
\]

Figure 12. A blame-exact result/term correspondence

4.2 Theorem [Semantic type soundness]:

1. If \( \Delta \vdash s_1 \triangleleft s_2 \) then \( \Delta \vdash \Gamma \models \Gamma \vdash s_1 \triangleleft s_2 \).
2. If \( \Delta \vdash s : S \) then \( \Delta \models \Gamma \models s : S \).
3. If \( \Delta \vdash \Gamma \models s \) then \( \Delta \vdash \Gamma \models s \).

The first part follows by induction on the subtyping judgment. However, we run into some complications with the second and third parts (which must be proven together). The crux of the difficulty lies with the \( \text{S_APP} \) rule. Suppose the application \( s_1 s_2 \) was well typed and \( s_1 \in \llbracket x : S_1 \rightarrow S_2 \rrbracket \) and \( s_2 \in \llbracket S_1 \rrbracket \). According to \( \text{S_APP} \), the application’s type is \( S_2 \llbracket x := s_2 \rrbracket \). By the type semantics defined in Figure 11, if \( s_1 \in \llbracket x : S_1 \rightarrow S_2 \rrbracket \), then \( s_1 q \in \llbracket S_2 \langle x := q \rangle \rrbracket \) for any \( q \in \llbracket S_1 \rrbracket \). Sadly, \( s_2 \) isn’t necessarily a result! We do know, however, that \( s_2 \in \llbracket S_1 \rrbracket \), so \( s_2 \rightarrow^* h q \) by strong normalization (Lemma 4.1). We need to ask, then, the type semantics of \( S_2 \llbracket x := s_2 \rrbracket \) and \( S_2 \llbracket x := q \rrbracket \) relate.

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 that allows redices 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 \( S_2 \llbracket x := s_2 \rrbracket \) and \( S_2 \llbracket x := q \rrbracket \)—have the same semantics (see the long version for details). The definition of parallel reduction is standard, though we need to be careful to make it respect our call-by-value reduction order: the \( \beta \)-redex \( \llbracket x : S_1, s_2 \rrbracket \) should not be contracted unless \( s_2 \) is a value, since doing so can change the order of effects. (Other redices within \( s_1 \) and \( s_2 \) can safely reduce.) The proof requires a longish sequence of technical lemmas that essentially show that \( \Rightarrow \) commutes with \( \rightarrow^* \). Since the proofs require fussy symbolic manipulation, we’ve done these proofs in Coq. Our development is available at http://www.cis.upenn.edu/~mgree/papers/ lambdah_parred.tgz.

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

Theorem 4.2 gives us type soundness, and it combines with Lemma 4.1 for an even stronger result: well-typed programs always evaluate to values of appropriate (semantic) type.

5. 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 12). We read \( t \sim s : T \) as “\( t \) corresponds with \( s \) at type \( T \)”. Terms corresponding at \( B \) both go to \( k \in \mathcal{K}_B \) or to \( \top l \).

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

The full definition of \( \phi \) is in Figure 14. One point to note is that, 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 \( T_{\text{VART}} \) and \( T_{\text{VARC}} \) 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 \( f : x : \text{Int} \mid \text{pos x} \rightarrow \{ y : \text{Int} \mid \text{true} \} \rightarrow \{ z : \text{Int} \mid f 0 = 0 \} \). Note that this contract is well-formed in \( \lambda_C \), but that the codomain “abuses” the bound variable. A naive translation \( f/0 \) will not be well-typed in \( \lambda_H \). To see why, consider the function \( \text{sqrt} : \text{Float} \rightarrow \text{Int} \), e.g., \( \text{sqrt}(\text{Float}) \rightarrow \text{Int} \). Since \( f \) only accepts positive arguments. The problem is that \( \text{SFV\_FUNC} \) can add a (possibly refined) type to the context when checking the codomain, so we need to restore the “variables have raw types” invariant. By tracking which variables were bound in contracts by \( \lambda_C \), we can be sure to cast them to raw types when they’re referenced. We therefore translate the contract above to \( f : S \rightarrow \{ x : \text{Int} \mid ((S \Rightarrow \{ \text{Int} \mid \text{Int} \}) f 0 = 0 \} \), where \( S = x : \text{Int} \mid \text{pos x} \rightarrow \{ z : \text{Int} \mid f 0 = 0 \} \). This (partially) motivates the \( x : c^{\text{ID}} \) binding form in dependent \( \lambda_C \).

Dual closing substitutions

\[
\Delta \vdash \Gamma \models \delta \iff
\begin{align*}
&\forall \Gamma. \Delta \vdash o \sim o' \vdash \Gamma. \delta(o) \sim \delta(o') \\
&\forall \Gamma. \delta(o) \models \delta(o')
\end{align*}
\]

\[\Gamma \models \delta \iff\begin{cases} \end{cases}\]

Figure 13. Blame-exact correspondence for \( \phi \) from picky \( \lambda_C \)
The translation \( \phi \) from dependent \( \lambda_C \) to dependent \( \lambda_H \)

inserted cast. It helps to think of polarity in terms of position rather than the presence or absence of a prime.

5.1 Theorem [Behavioral correspondence]: If \( \Gamma \vdash t : T \), then:
1. If \( \Gamma \vdash t : T \) is \( s \) then \( \Gamma \vdash c \rightarrow s : T \).
2. If \( \Gamma \vdash c \rightarrow s : T \) then \( \Gamma \vdash c \rightarrow l \rightarrow s : T \).

We can now prove that \( \phi \) preserves types, using Theorem 5.1 to show that \( \phi \) preserves the implication judgment.

5.2 Theorem [Type preservation]: If \( \phi(\Gamma) = \Delta \), then:
1. If \( \Gamma \vdash t : T \) is \( s \) then \( \Gamma \vdash [t] : [T] \).
2. If \( \Gamma \vdash [t] : [T] \) is \( s \) then \( \Gamma \vdash c \rightarrow [s] : [T] \).
3. If \( \Gamma \vdash c \rightarrow [s] : [T] \) is \( s \) then \( \Gamma \vdash [l] : [T] \).

5.2 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 sketch proofs that \( \psi \) is type preserving and induces behavioral correspondence.

The full definition of \( \psi \) is in Figure 15. 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_CDECOMP. Since \( \psi \) inserts new casts, we need to pick a blame label: \( \psi([S_1 \Rightarrow S_2]) \) passes \( l \) as an index to \( \psi([S_1, S_2]) \).

We reuse the term correspondence \( t \sim s : T \) (Figure 12) and define a new contract/cast correspondence \( c \sim S_1 \Rightarrow S_2 : T \) (Figure 16), relating contracts and pairs of \( \lambda_H \) types. This correspondence uses the term correspondence in the base type case and follows the pattern of F_CDECOMP in the function case. Since it inserts a cast in the function case, we index the relation with a label, just like \( \psi \). We define closing substitutions ignoring the contracts in the context; we lift the relation to open terms in the standard way.

We first show that \( s \) and \( \psi(s) \) behaviorally correspond, and then we can prove that \( \psi \) is type preserving, using the behavioral correspondence to show that \( \psi \) preserves implication.

5.3 Theorem [Behavioral correspondence]:
1. If \( \Delta \vdash s : S \) then \( [\Delta] \vdash [s] : [S] \).
2. If \( \Delta \vdash S_1 \) and \( \Delta \vdash S_2 \), where \( [S_1] = [S_2] = [S] \), then \( [\Delta] \vdash [\psi(S_1, S_2)] \Rightarrow s \Rightarrow S_2 : [S] \) (for all \( l \)).

5.4 Theorem [Type preservation for \( \psi \)]:
1. If \( \Delta \vdash s : S \) then \( [\Delta] \vdash [s] : [S] \).
2. If \( \Delta \vdash S_1 \) and \( \Delta \vdash S_2 \), where \( [S_1] = [S_2] = [T] \), then \( [\Delta] \vdash [\psi(S_1, S_2)] \Rightarrow S_1 \Rightarrow S_2 : [T] \).

6. 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.

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

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 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 \( \tau \)_VARC derivations).

We can show the behavioral correspondence using a blame-inexact logical relation, defined in Figure 17. The behavioral corre-
\textbf{Value correspondence}\n\[ k \approx_r k : B \iff k \in \mathcal{K}_B \]
\[ v \approx_r w : T_1 \rightarrow T_2 \iff \forall t \approx_r s : T_1, v t \approx_r w s : T_2 \]

\textbf{Term correspondence}\n\[ t \approx_r s : T \iff s \xrightarrow{\lambda} \top \lor (t \xrightarrow{\lambda} v \land s \xrightarrow{\lambda} w \lor v \approx_r w : T) \]

\textbf{Contract / type correspondence}\n\[ \{x : B \mid t\} \approx_r \{x : B \mid s\} : B \iff \forall k \in \mathcal{K}_B, t(x := k) \approx_r s(x := k) : \text{Bool} \]
\[ x : c_1 \rightarrow c_2 \approx_r x : S_1 \rightarrow S_2 : T_1 \rightarrow T_2 \iff c_1 \approx_r S_1 \Rightarrow T_1 \land \forall t \approx_s s : T_1, c_2(x := t) \approx_r S_2(x := s) : T_2 \]

\textbf{Dual closing substitutions}\n\[ \Gamma \models \delta \iff \forall x \in \text{dom}(\Gamma), \delta(x) \approx \delta_2(x) : [\Gamma(x)] \]

\textbf{Figure 17. Blame-inexact correspondence for }\phi\textbf{ from lax }\lambda_c\textbf{.}

\textbf{6.1 Lemma [Extra casts]:} If \( t \sim_r s : T \) and \( c_1 \sim_r S_1 : T \) and \( c_2 \sim_r S_2 : T \), then \( t \sim_r (S_1 \Rightarrow S_2)^l s : T \).

\textbf{6.2 Theorem [Behavioral correspondence]:} If \( \vdash \Gamma \), then:
1. If \( \phi(\Gamma \vdash t : T) = s \) then \( \Gamma \vdash t \sim_r s : T \).
2. If \( \phi(\Gamma \vdash c : T) = S \) then \( \Gamma \vdash c \sim_r S : T \).

\textbf{6.3 Theorem [Type preservation]:} For programs without active checks, if \( \phi(\Gamma) = \Delta \), then:
1. \( \vdash \Delta \).
2. \( \Delta \vdash \phi(\Gamma \vdash t : T) : [T] \).
3. \( \Delta \vdash \phi(\Gamma \vdash c : T) \).

\textbf{Contract / type correspondence}\n\[ \{x : B \mid t\} \sim_r \{x : B \mid s\} \Rightarrow \{x : B \mid s_2\} : B \iff \forall k \in \mathcal{K}_B, t(x := k) \sim_r s_2(x := k) : \text{Bool} \]
\[ x : c_1 \rightarrow c_2 \sim_r x : S_1 \rightarrow S_2 \Rightarrow x : S_21 \rightarrow S_22 : T_1 \rightarrow T_2 \iff c_1 \sim_r S_1 \Rightarrow T_1 \land \forall t \sim_s s : T_1, c_2(x := t) \sim_r S_22(x := s) : T_2 \]

\textbf{Dual closing substitutions}\n\[ \Gamma \models \delta \iff \forall x \in \text{dom}(\Gamma), \delta(x) \sim \delta_2(x) : [\Gamma(x)] \]

\textbf{Figure 18. Blame-inexact correspondence for }\psi\textbf{ into picky }\lambda_c\textbf{.}

While its translation goes to blame. In the first example, blame is raised in \( \Lambda_0 \) due to bulkproofing. In the second, blame is raised due to the extra cast from the translation of T_VARC. For the first, let
\[ c = f : (\{x : \text{Int} \mid \text{true}\} \rightarrow \{y : \text{Int} \mid \text{nonzero}\} ) \rightarrow \{z : \text{Int} \mid f(0) = 0\} \]
\[ S_1 = x : \{x : \text{Int} \mid \text{true}\} \rightarrow \{y : \text{Int} \mid \text{nonzero}\} \]
\[ S = \phi(\{l \rightarrow c\} : (\text{Int} \rightarrow \text{Int}) \rightarrow \text{Int}) \]
\[ = f : S_1 \rightarrow \{z : \text{Int} \mid ((S_1 \Rightarrow S_1)^l) f(0) = 0\} \]

We find \( (c_1)^l \Rightarrow (\lambda f, 0) (\lambda x, 0) \sim_r 0 \) but \( (\lambda x : [c]) \sim_r S \Rightarrow [S] \).

\textbf{6.2 Translating }\Lambda_0\textbf{ to picky }\lambda_c\textbf{.}

Terms in \( \Lambda_0 \) and their }\psi\textbf{-images in lax }\lambda_c\textbf{ correspond exactly, as shown Section 5.2. When we change the operational semantics of }\lambda_c\textbf{ to be }picky\textbf{, however, }\psi\textbf{-}(s)\textbf{ blames (strictly) more often than }s\textbf{. Nevertheless, we can show an inexact correspondence, as we did for }\phi\textbf{ and lax }\lambda_c\textbf{ in Section 6.1. We use a logical relation }\sim_r\textbf{ similar to }\sim_r\textbf{, used for }\phi\textbf{ into lax }\lambda_c\textbf{ (Figure 17), though we reverse the asymmetry, allowing picky }\lambda_c\textbf{ to blame more than }\Lambda_0\textbf{. The proof follows the same general pattern: we first show that it is safe to add extra contract checks, then the correspondence for well-typed terms. We can also show type preservation for source programs (excluding active checks).}

\textbf{6.4 Lemma [Extra contracts]:} If \( t \sim_r s : T \) and \( c \sim_r S_1 \Rightarrow S_2 : T \) then \( (c)^l \Rightarrow t \sim_r s : T \).

\textbf{6.5 Theorem [Behavioral correspondence]:}
1. If \( \Delta \vdash s : S \) then \( [\Delta] \vdash \psi(s) \sim_r s : [S] \).
2. If \( \Delta \vdash S_1 \) and \( \Delta \vdash S_2 \), where \( [S_1] = [S_2] = [S] \), then \( [\Delta] \vdash \psi(S_1, S_2) \sim_r S_1 \Rightarrow S_2 : [S] \).

\textbf{6.6 Theorem [Type preservation for }\psi\textbf{]:} For programs without active checks, if \( \Gamma \vdash \Delta \), 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 \( [\Delta] \vdash \psi(S_1, S_2) : T \).
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:

$$
S_1 = \lambda s_1. \lambda s_2. f(s_1) \rightarrow \{ y : \text{Int} \mid \text{nonzero } y \} \rightarrow \text{Int}
\quad \text{and} \quad
S_2 = \lambda s_1. \lambda s_2. f(s_1) \rightarrow \{ z : \text{Int} \mid f \circ 0 = 0 \}
$$

The main 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 call-by-value 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 [2009], which uses full $\beta$-reduction (more on this below).

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 Gronski and Flanagan [2007] and Flanagan [2006], the operational semantics checks casts “all in one go”:

$$
\begin{align*}
\text{sg} \langle x : 0 \rangle \rightarrow \text{true} \\
\langle \{ x : B \mid s_1 \} \Rightarrow \{ x : B \mid s_2 \} \rangle\langle k \rangle \\
\rightarrow_h k
\end{align*}
$$

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 Gronski and Flanagan [2007] and Flanagan [2006] involve a circularity between the typing, subtyping, and implication relations. Knowles and Flanagan [2009] 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 meta-theory of dependent $\lambda_C$. (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 nondependent 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 theirs. Our $\psi$ translation completes their story for the nondependent 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 [2009], 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 (though not the earlier one of Gronski and Flanagan), 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, non-deterministic $\beta$-reduction, rather than specifying a particular order of reduction, as we have done. This significantly simplifies parts of the meta-theory by allowing them to avoid introducing parallel reduction. We prefer standard call-by-value reduction because we consider blame as an exception—a computational effect—and we want to be able to reason about whether blame will be raised by expressions involving many casts.

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 Figure 19—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 $\lambda_{\text{com}}$ [Findler and Felleisen 2002], though our presentation is slightly different in its use of checks. Hinze et al. [2006] adapted Findler and Felleisen-style contracts to a location-passing implementation in Haskell, using a picky dependent function contract rule.

Our $\lambda_H$ type semantics in Section 4 is effectively a semantics of contracts. Blume and McAllester [2006] offers 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.

We have discussed only a small sample of the many papers on contracts and related ideas. We refer the reader to Knowles and Flanagan [2009] for a more comprehensive survey.
<table>
<thead>
<tr>
<th></th>
<th>FF02 (1)</th>
<th>HJL06 (2)</th>
<th>GF07 λc (3)</th>
<th>BM06 (4)</th>
<th>our λc (5)</th>
<th>GF07 λH (6)</th>
<th>F06 (7)</th>
<th>KF09 (8)</th>
<th>WF09 (9)</th>
<th>OTMW04 (10)</th>
<th>our λH (11)</th>
</tr>
</thead>
<tbody>
<tr>
<td>dep (9)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</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>
<td>CBV</td>
<td>CBV</td>
<td>CBV</td>
<td>CBV</td>
<td>CBV</td>
</tr>
<tr>
<td>blame (12)</td>
<td>⊥</td>
<td>⊥</td>
<td>⊥</td>
<td>⊥ or ⊥</td>
<td>⊥</td>
<td>⊥</td>
<td>⊥</td>
<td>⊥ active</td>
<td>⊥ active</td>
<td>⊥ active</td>
<td>⊥ active</td>
</tr>
<tr>
<td>checking (13)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>typing (14)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>any con (15)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Figure 19. Comparison of related systems

(1) Findler and Felleisen [2002], (2) Hinze et al. [2006], (3) Gronski and Flanagan [2007], (4) Blume and McAllester [2006], (5) Flanagan [2006], (6) Knowles and Flanagan [2009], (7) Wadler and Findler [2009], (8) Ou et al. [2004], (9) Does the system include dependent contracts or function types (√) or not (×) and, for latent systems, is the semantics lax or picky? (10) An “unusual” form of dependency, where negative blame in the codomain results in nontermination. (11) A nondeterministic variant of CBV. (12) Do failed contracts raise labeled blame (⇑), raise blame without a label (⇑), get stuck, or sometimes raise blame and sometimes diverge (⊥)? (13) 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 (⊂)? (14) Is the typing relation well defined (i.e., for dependently typed systems, is it based on a type semantics or, as in WF09, a “tagging” scheme), or is the definition circular? (15) Are arbitrary user-defined boolean functions allowed as contracts or refinements (√), or only built-in ones (×)?

8. Future work

Our calculi are strongly normalizing; extending our results to systems that allow recursion is a natural next step. The changes seem nontrivial: with nontermination, inexact correspondences must allow not only more blame, but also more nontermination—each extra check is another opportunity for divergence.

Most studies of contracts, including ours, only allow refinements of base types; however, Blume and McAllester [2006] and Xu et al. [2009] also allow refinements of functions. This extension seems needed if contracts are to be combined with polymorphism, since in this setting we may want to refine type variables, which may later be substituted with types involving functions. We conjecture that dependent λH with function refinements is sound, but it is not clear how the translations will need to be modified.

Acknowledgments

Sewell and Zappa Nardelli’s OTT tool was invaluable for organizing our definitions. We used Aydemir and Weirich’s LNGen tool for the Coq development of parallel reduction. Brian Aydemir, João Belo, Chris Casinghino, Nate Foster, and the POPL reviewers gave us helpful comments. Our work has been supported by the National Science Foundation under grants 0702545 A Practical Dependent-Type Functional Programming Language, 0910786 TRELLYS, 0534592, Linguistic Foundations for XML View Update and 0915671, Contracts for Precise Types.

References

Philip Wadler and Robert Bruce Findler. Well-typed programs can’t be blamed. In European Symposium on Programming (ESOP), pages 1–16, 2009.