Well-typed programs can't be blamed

Philip Wadler Robert Bruce Findler

This is the Technical Report version of the 2009 ESOP paper by the same title. It includes the ESOP version verbatim, followed by an appendix containing proofs.

Contents

Well-typed programs can't be blamed

Philip Wadler[1] and Robert Bruce Findler[2]

[1] University of Edinburgh
[2] University of Chicago

Abstract. We introduce the *blame calculus*, which adds the notion of blame from Findler and Felleisen's *contracts* to a system similar to Siek and Taha's *gradual types* and Flanagan's *hybrid types*. We characterise where positive and negative blame can arise by decomposing the usual notion of subtype into positive and negative subtypes, and show that these recombine to yield naive subtypes. Naive subtypes previously appeared in type systems that are unsound, but we believe this is the first time naive subtypes play a role in establishing type soundness.

1 Introduction

Much recent work has focused on integrating dynamic and static typing using *contracts* [4] to ensure that dynamically-typed code meets statically-typed invariants. Examples include *gradual types* [15], *hybrid types* [5, 8], *dynamic dependent types* [13], and *multi-language programming* [10]. Both Meijer [11] and Bracha [2] argue in favor of mixing dynamic and static typing. Static and dynamic typing are both supported in Visual Basic, and similar integration is planned for Perl 6 and ECMAScript 4.

Here we unify some of this work, by introducing a notion of blame (from contracts) into a type system with casts (similar to intermediate languages for gradual and hybrid types), yielding a system we dub the *blame calculus*. In this calculus, programmers may add casts to evolve dynamically typed code into statically typed, (as with gradual types) or to evolve statically typed code to use subset types (as with hybrid types).

The technical content of this paper is to introduce notions of positive and negative subtypes, and prove a theorem that characterises when positive and negative blame can occur. A corollary is that when a program integrating less-typed and more-typed components goes wrong the blame must lie with the less-typed component. Though obvious, this result has either been ignored in previous work or required a complex proof; here we give a simple proof.

Our work involves both ordinary subtypes (which, for functions, is contravariant in the domain and covariant in the range) and naive subtypes (which is covariant in both the domain and the range). Ordinary subtypes characterize a cast that cannot fail, while naive subtypes characterize which side of a cast is less typed (and hence will be blamed if the cast fails). We show that ordinary subtypes decompose into positive and negative subtypes, and that these recombine in a different way to yield naive subtypes. A striking analogy is a tangram, where a square decomposes into parts that recombine into a different shape (see Figure 1). Naive subtypes previously appeared in type systems that are unsound, notably that of Eiffel [12], but we believe this is the first time naive subtypes play a role in establishing type soundness.

Gradual types [15], hybrid types [5, 8], and dynamic dependent types [13] use source languages where most or all casts are omitted, but inferred by a type-directed translation; all three use similar translations which target similar intermediate languages. The blame calculus resembles these intermediate languages. Our point is that the intermediate language is in itself suitable as a source language, with the advantage that it becomes crystal clear where static guarantees hold and where dynamic checks are enforced.

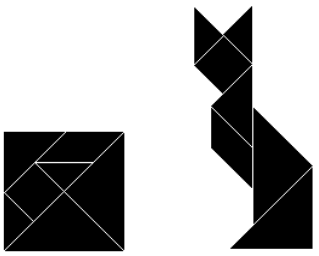

Fig. 1. Tangram as metaphor: Ordinary subtyping decomposes and recombines to yield naive subtyping.

The blame calculus uses subset types as found in hybrid types and dynamic dependent types, but it lacks the dependent function types found in these systems (an important area for future work). Hybrid types and dynamic dependent types are parameterized by a theorem prover, which returns true, false, or maybe when supplied with a logical implication required by a subtyping relationship; the blame calculus corresponds to the extreme case where the theorem prover always returns maybe.

We make the following contributions.

- We introduce the blame calculus, showing that a language with explicit casts is suited to many of the same purposes as gradual types and hybrid types (Section 2).
- We give a framework similar to that of hybrid types and dynamic dependent types, but with a decidable type system for the source language (Section 3).
- We factor ordinary subtypes positive and negative subtypes, which recombine into naive subtypes. We prove that a cast from a positive subtype cannot give rise to positive blame, and that a cast from a negative subtype cannot give rise to negative blame (Section 4).

An earlier version of this paper appeared in a workshop [19]. The current version is completely rewritten and some technicalities differ. A rule merging positive blame and negative blame from distinct casts has been eliminated, and as a consequence we use a simpler notation with one label rather than two. A rule making every ground type a subtype of type `Dyn` has been added, making the subtyping relations less conservative. Detailed proofs may be found in the accompanying technical report [20].

2 The blame calculus

2.1 From untyped to typed

Figure 2 presents a series of example programs, which we consider in turn.

Program (a) is untyped. By default, our programming language is typed, so we indicate untyped code by surrounding it with ceiling brackets. Untyped code is really uni-typed (a slogan due to Robert Harper); it is a special case of typed code where every term has type `Dyn`. Here the term evaluates to $\lceil 4 \rceil : \texttt{Dyn}$.

As a matter of software engineering, when we add types to our code we may not wish to do so all at once. Progam (b) contains typed and untyped parts, fit together

(a) $\lceil \texttt{let}\ x = 2$
$\quad \texttt{let}\ f = \lambda y.\ y + 1$
$\quad \texttt{let}\ h = \lambda g.\ g\ (g\ x)$
$\quad \texttt{in}\ h\ f \rceil$

(b) $\texttt{let}\ x = 2$
$\quad \texttt{let}\ f = \langle \texttt{Int} \to \texttt{Int} \Leftarrow \texttt{Dyn} \rangle^p\ \lceil \lambda y.\ y + 1 \rceil$
$\quad \texttt{let}\ h = \lambda g : \texttt{Int} \to \texttt{Int}.\ g\ (g\ x)$
$\quad \texttt{in}\ h\ f$

(c) $\texttt{let}\ x = \langle \texttt{Nat} \Leftarrow \texttt{Int} \rangle^p\ 2$
$\quad \texttt{let}\ f = \langle \texttt{Nat} \to \texttt{Nat} \Leftarrow \texttt{Int} \to \texttt{Int} \rangle^q\ (\lambda y : \texttt{Int}.\ y + 1)$
$\quad \texttt{let}\ h = \lambda g : \texttt{Nat} \to \texttt{Nat}.\ g\ (g\ x)$
$\quad \texttt{in}\ \ h\ f$

(d) $\texttt{let}\ x = \lceil \texttt{true} \rceil$
$\quad \texttt{let}\ f = \lambda y : \texttt{Int}.\ y + 1$
$\quad \texttt{let}\ h = \langle (\texttt{Int} \to \texttt{Int}) \to \texttt{Int} \Leftarrow \texttt{Dyn} \rangle^p\ \lceil \lambda g.\ g\ (g\ x) \rceil$
$\quad \texttt{in}\ h\ f$

(e) $\texttt{let}\ x = \lceil \texttt{true} \rceil$
$\quad \texttt{let}\ f = \langle \texttt{Dyn} \Leftarrow \texttt{Int} \to \texttt{Int} \rangle^p\ (\lambda y : \texttt{Int}.\ y + 1)$
$\quad \texttt{let}\ h = \lceil \lambda g.\ g\ (g\ x) \rceil$
$\quad \texttt{in}\ \lceil h\ f \rceil$

(f) $\texttt{let}\ x = \langle \texttt{Nat} \Leftarrow \texttt{Int} \rangle^p\ 3$
$\quad \texttt{let}\ f = \langle \texttt{Nat} \to \texttt{Nat} \Leftarrow \texttt{Int} \to \texttt{Int} \rangle^q\ (\lambda y : \texttt{Int}.\ y - 2)$
$\quad \texttt{let}\ h = \lceil \lambda g.\ g\ (g\ x) \rceil$
$\quad \texttt{in}\ \lceil h\ f \rceil$

Fig. 2. Example programs

by casting the untyped code to a suitable type. and the term evaluates to $4 : \texttt{Int}$. Gradual evolution is overkill for such a short piece of code, but in real systems it plays an important role [17, 18]. Here $\lceil \lambda y.\ y + 1 \rceil$ has type $\texttt{Dyn}$, and the cast converts it to type $\texttt{Int} \to \texttt{Int}$.

In general, a cast from source type S to target type T is written $\langle T \Leftarrow S \rangle^p\ s$, where subterm s has type S and the whole term has type T, and p is a *blame label*. We assume an involutive operation of negation on blame labels: if p is a blame label then $\bar{p}$ is its negation, and $\overline{\bar{p}}$ is the same as p. Consider a cast with blame label p: blame is allocated to p when the *term contained* in the cast fails to satisfy the contract associated with the cast, while blame is allocated to $\bar{p}$ when the *context containing* the cast fails to satisfy the contract.

Our notation is chosen for clarity rather than compactness. Writing the source type is redundant, but convenient for a core calculus. Our notation is based on that of Gronski and Flanagan [7].

2.2 Contracts and subset types

Findler and Felleisen [4] introduced higher-order contracts, and Flanagan [5] and Ou *et al.* [13] observed that contracts can be incorporated into a type system as a form of *subset* (or *refinement*) type. An example is $\{x : \texttt{Int} \mid x \geq 0\}$, the type of all integers greater than zero, which we will write $\texttt{Nat}$. A cast from $\texttt{Int}$ to $\texttt{Nat}$ performs a dynamic test, checking that the integer is indeed greater than or equal to zero. Just as

we can start with an untyped program and add types, we can start with a typed program and add subset types. Program (c) is a version of the previous program with subset types added.

Unlike hybrid or dependent types, the blame calculus does not require subsumption. As a technical nicety, this allows us to design a type system which (like gradual types) satisfies *unicity*: every well-typed term has exactly one type. In order to achieve unicity, we must add new value forms corresponding to the result of casting to a subset type. Thus, the value of Program (c) is not $4 : \texttt{Int}$ but $4_{\texttt{Nat}} : \texttt{Nat}$.

2.3 The blame game

The above examples execute with no errors, but in general we may not be so lucky. Casts perform dynamic tests at run-time that fail if a value cannot be coerced to the given type. A cast to a subset type reduces to a dynamic test of the condition on the type. Recall that `Nat` denotes $\{x : \texttt{Int} \mid x \geq 0\}$. Here is a successful test:

$$\langle \texttt{Nat} \Leftarrow \texttt{Int} \rangle^p \, 4 \quad \longrightarrow \quad 4 \geq 0 \; \rhd^p \; 4_{\texttt{Nat}} \quad \longrightarrow \quad \texttt{true} \; \rhd^p \; 4_{\texttt{Nat}} \quad \longrightarrow \quad 4_{\texttt{Nat}}$$

And here is a failed test:

$$\langle \texttt{Nat} \Leftarrow \texttt{Int} \rangle^p \, -4 \quad \longrightarrow \quad -4 \geq 0 \; \rhd^p \; -4_{\texttt{Nat}} \quad \longrightarrow \quad \texttt{false} \; \rhd^p \; -4_{\texttt{Nat}} \quad \longrightarrow \quad \Uparrow p$$

The middle steps show a new term form that performs a dynamic test, of the form $s \rhd^p v_{\{x:B|t\}}$. If s evaluates to true, the value of subset type is returned; if s evaluates to false, blame is allocated to p, written $\Uparrow p$.

Given an arbitrary term that takes integers to integers, it is not decidable whether it also takes naturals to naturals. Therefore, when casting a function type the test is deferred until the function is applied. This is the essence of higher-order contracts.

Here is an example of casting a function and applying the result.

$$\begin{array}{l}
(\langle \texttt{Nat} \to \texttt{Nat} \Leftarrow \texttt{Int} \to \texttt{Int} \rangle^p \, (\lambda y : \texttt{Int}.\; y + 1)) \, 2_{\texttt{Nat}} \longrightarrow \\
\langle \texttt{Nat} \Leftarrow \texttt{Int} \rangle^p ((\lambda y : \texttt{Int}.\; y + 1) \, (\langle \texttt{Int} \Leftarrow \texttt{Nat} \rangle^{\bar{p}} \, 2_{\texttt{Nat}}) \longrightarrow \\
\langle \texttt{Nat} \Leftarrow \texttt{Int} \rangle^p \, ((\lambda y : \texttt{Int}.\; y + 1) \, 2) \longrightarrow \\
\langle \texttt{Nat} \Leftarrow \texttt{Int} \rangle^p \, 3 \longrightarrow 3_{\texttt{Nat}}
\end{array}$$

The cast on the function breaks into two casts, each in opposite directions: the cast on the result takes the range of the *source* to the range of the *target*, while the cast on the argument takes the domain of the *target* to the domain of the *source*. Preserving order for the range while reversing order for the domain is analogous to the standard rule for function subtyping, which is covariant in the range and contravariant in the domain.

Observe that the blame label on the reversed cast has been negated, because if that cast fails it is the fault of the context, which supplies the argument to the function. Conversely, the blame label is not negated on the result cast, because if that cast fails it is the fault of the function itself.

The above cast took a function with range and domain `Int` to a function with more precise range and domain `Nat`. Now consider a cast to a function with less precise range and domain `Dyn`.

$$\begin{array}{l}
(\langle \texttt{Dyn} \to \texttt{Dyn} \Leftarrow \texttt{Int} \to \texttt{Int} \rangle^p \, (\lambda y : \texttt{Int}.\; y + 1)) \, \lceil 2 \rceil \longrightarrow \\
\langle \texttt{Dyn} \Leftarrow \texttt{Int} \rangle^p ((\lambda y : \texttt{Int}.\; y + 1) \, (\langle \texttt{Int} \Leftarrow \texttt{Dyn} \rangle^{\bar{p}} \, \lceil 2 \rceil)) \longrightarrow \\
\langle \texttt{Dyn} \Leftarrow \texttt{Int} \rangle^p ((\lambda y : \texttt{Int}.\; y + 1) \, 2) \longrightarrow \langle \texttt{Dyn} \Leftarrow \texttt{Int} \rangle^p \, 3 \longrightarrow \lceil 3 \rceil
\end{array}$$

Again, a cast on the function breaks into two casts, each in opposite directions.

If we consider a well-typed term of the form

$$(\langle \texttt{Nat} \to \texttt{Nat} \Leftarrow \texttt{Int} \to \texttt{Int} \rangle^p \, f) \, x$$

we can see that negative blame *never* adheres to this cast, because the type checker guarantees that x has type `Nat`, and the cast from `Nat` to `Int` always succeeds. However positive blame may adhere, for instance if f is $\lambda y : \texttt{Int}.\ y - 2$ and x is 1.

Conversely, if we consider a well-typed term of the form

$$(\langle \texttt{Dyn} \to \texttt{Dyn} \Leftarrow \texttt{Int} \to \texttt{Int} \rangle^p \, f) \, x$$

we can see that positive blame *never* adheres to this cast, because the types guarantee that f returns an `Int`, and the cast from `Int` to `Dyn` always succeeds. However negative blame may adhere, for instance if f is $\lambda y : \texttt{Int}.\ y + 1$ and x is $\lceil \texttt{true} \rceil$.

The key result of this paper is to show that casting from a more precise type to a less precise type cannot give rise to positive blame (but may give rise to negative); and that casting for a less precise type to a more precise type cannot give rise to negative blame (but may give rise to positive). Here are the two examples considered above, with the more precise type on the left, and the less precise type on the right.

$$\texttt{Nat} \to \texttt{Nat} <:_n \texttt{Int} \to \texttt{Int} \qquad\qquad \texttt{Int} \to \texttt{Int} <:_n \texttt{Dyn} \to \texttt{Dyn}$$

We call this *naive* subtyping (hence the subscript n) because it is covariant in both the domain and the range of function types, in contrast to traditional subtyping, which is contravariant in the domain and covariant in the range. We formally define both subtyping and naive subtyping in Section 3.3.

2.4 Well-typed programs can't be blamed

Consider a program that mixes typed and untyped code; it will contain two sorts of casts. One sort gives types to untyped code. Such casts make types more precise, and so cannot give rise to negative blame. For instance, Program (d) in Figure 2 fails blaming p. Because the blame is positive, the fault lies with the untyped code inside the cast.

The other sort takes typed code and makes it untyped. Such a cast makes types less precise, and so cannot give rise to positive blame. For instance, Program (e) fails blaming $\bar{p}$. Because the blame is negative, the fault lies with the code outside the cast.

Both times the fault lies with the untyped code! This is of course what we would expect, since typed code should contain no type errors. Understanding positive and negative blame, and knowing when each can arise, is the key to giving a simple proof of this expected fact.

The same analysis generalizes to code containing subset types. For instance, Program (f) fails blaming q. In this case, both casts make the types more precise, so cannot give rise to negative blame. Because the blame is positive, the fault lies with the less refined code inside the cast.

3 Types, reduction, subtyping

Compile-time type rules of our system are presented in Figure 3, run-time type rules and reduction rules in Figure 4, and rules for subtyping in Figure 5. We discuss each of these in turn in the following three subsections.

Syntax

variables	x, y	blame labels	p, q
base types	B	$::= \texttt{Bool} \mid \texttt{Int} \mid \cdots$	
constants	c	$::= \texttt{true} \mid \texttt{false} \mid 0 \mid 1 \mid \cdots \mid + \mid - \mid \geq \cdots$	
types	S, T	$::= \texttt{Dyn} \mid B \mid S \to T \mid \{x : B \mid t\}$	
terms	s, t, u	$::= x \mid c \mid \lambda x : S.\ t \mid t\ s \mid \langle T \Leftarrow S \rangle^p\ s$	

Compile-time typing $\boxed{\Gamma \vdash t : T}$

$$\frac{x : T \in \Gamma}{\Gamma \vdash x : T} \qquad \frac{T = \text{ty}(c)}{\Gamma \vdash c : T}$$

$$\frac{\Gamma,\, x : S \vdash t : T}{\Gamma \vdash \lambda x : S.\ t : S \to T} \qquad \frac{\Gamma \vdash t : S \to T \qquad \Gamma \vdash s : S}{\Gamma \vdash t\ s : T} \qquad \frac{\Gamma \vdash s : S \qquad S \sim T}{\Gamma \vdash \langle T \Leftarrow S \rangle^p\ s : T}$$

Compatibility $\boxed{S \sim T}$

$$B \sim B \qquad \texttt{Dyn} \sim T \qquad S \sim \texttt{Dyn}$$

$$\frac{S \sim S' \qquad T \sim T'}{S \to T \sim S' \to T'} \qquad \frac{B \sim T}{\{x : B \mid s\} \sim T} \qquad \frac{S \sim B}{S \sim \{y : B \mid t\}}$$

Fig. 3. Compile-time types

3.1 Types and terms

Figure 3 presents the syntax of types and terms and the compile-time type rules. The language is explicitly and statically typed. (See Section 3.4 for embedding untyped terms.)

We let S, T range over types, and s, t range over terms. A type is either a base type B, the dynamic type $\texttt{Dyn}$, a function type $S \to T$, or a subset type $\{x : B \mid t\}$. A term is either a variable x, a constant c, a lambda expression $\lambda x : S.\ t$, an application $s\ t$, or a cast expression $\langle T \Leftarrow S \rangle^p\ s$. We write $\texttt{let}\ x = s\ \texttt{in}\ t$ as an abbreviation for $(\lambda x : S.\ t)\ s$ where s has type S.

We assume a denumerable set of constants. Every constant c is assigned a unique type $\text{ty}(c)$. We assume $\texttt{Bool}$ is a base type with $\texttt{true}$ and $\texttt{false}$ as constants of type $\texttt{Bool}$; and that $\texttt{Int}$ is a base type with 0, 1, and so on, as constants of type $\texttt{Int}$, and $+$ and $-$ as constants of type $\texttt{Int} \to \texttt{Int} \to \texttt{Int}$, and $\geq$ as a contant of type $\texttt{Int} \to \texttt{Int} \to \texttt{Bool}$, and possibly other constants. Constants must have base type or function type; this guarantees that every value of type $\texttt{Dyn}$ has the form $\texttt{Dyn}_G(v)$ and that every value of subset type has the form $v_{\{x:B|t\}}$. Constants of function type must not raise blame when evaluated; this guarantees that only casts can raise blame.

The type system is explained in terms of three judgements, which are presented in Figure 3. We write $\Gamma \vdash t : T$ if term t has type T in environment Γ, and we write $S \sim T$ if type S is compatible with type T. We let Γ range over type environments, which are a list of variable-type pairs $x : T$.

A type is well-formed if for every subset type $\{x : B \mid t\}$ we have that t has type $\texttt{Bool}$ on the assumption that x has type B (no other free variables may appear in t). In what follows, we assume all types are well-formed. We call B the *domain* of the subset type $\{x : B \mid t\}$.

Syntax

ground types	G	$::= B \mid \texttt{Dyn} \to \texttt{Dyn}$
terms	s, t, u	$::= \cdots \mid \texttt{Dyn}_G(v) \mid v_{\{x:B\mid t\}} \mid s \rhd^p v_{\{x:B\mid t\}}$
values	v, w	$::= x \mid c \mid \lambda x : S.\ t \mid \langle S' \to T' \Leftarrow S \to T\rangle^p\ v \mid \texttt{Dyn}_G(v) \mid v_{\{x:B\mid t\}}$
results	r	$::= t \mid \Uparrow p$
eval contexts	E	$::= [\,] \mid E\ s \mid v\ E \mid \langle T \Leftarrow S\rangle^p\ E \mid E \rhd^p v_{\{x:B\mid t\}}$

Run-time typing $\boxed{\Gamma \vdash t : T}$

$$\frac{\Gamma \vdash s : \texttt{Bool} \qquad \Gamma \vdash v : B \qquad t[x := v] \longrightarrow^* s}{\Gamma \vdash s \rhd^p v_{\{x:B\mid t\}} : \{x : B \mid t\}}$$

$$\frac{\Gamma \vdash v : G}{\Gamma \vdash \texttt{Dyn}_G(v) : \texttt{Dyn}} \qquad \frac{\Gamma \vdash v : B \qquad t[x := v] \longrightarrow^* \texttt{true}}{\Gamma \vdash v_{\{x:B\mid t\}} : \{x : B \mid t\}}$$

Reductions $\boxed{s \longrightarrow r}$

$$E[c\ v] \longrightarrow E[[\![c]\!](v)] \tag{1}$$
$$E[(\lambda x : S.\ t)\ v] \longrightarrow E[t[x := v]] \tag{2}$$
$$E[\langle B \Leftarrow B\rangle^p\ v] \longrightarrow E[v] \tag{3}$$
$$E[(\langle S' \to T' \Leftarrow S \to T\rangle^p\ v)\ w] \longrightarrow E[\langle T' \Leftarrow T\rangle^p\ (v\ (\langle S \Leftarrow S'\rangle^{\bar{p}}\ w))] \tag{4}$$
$$E[\langle \texttt{Dyn} \Leftarrow \texttt{Dyn}\rangle^p\ v] \longrightarrow E[v] \tag{5}$$
$$E[\langle \texttt{Dyn} \Leftarrow B\rangle^p\ v] \longrightarrow E[\texttt{Dyn}_B(v)] \tag{6}$$
$$E[\langle \texttt{Dyn} \Leftarrow S \to T\rangle^p\ v] \longrightarrow E[\texttt{Dyn}_{\texttt{Dyn}\to\texttt{Dyn}}(\langle \texttt{Dyn} \to \texttt{Dyn} \Leftarrow S \to T\rangle^p\ v)] \tag{7}$$
$$E[\langle T \Leftarrow \texttt{Dyn}\rangle^p\ \texttt{Dyn}_G(v)] \longrightarrow E[\langle T \Leftarrow G\rangle^p\ v], \quad \text{if } G \sim T \tag{8}$$
$$E[\langle T \Leftarrow \texttt{Dyn}\rangle^p\ \texttt{Dyn}_G(v)] \longrightarrow \Uparrow p, \quad \text{if } G \not\sim T \tag{9}$$
$$E[\langle \{x : B \mid t\} \Leftarrow S\rangle^p\ v] \longrightarrow E[\texttt{let}\ x = \langle B \Leftarrow S\rangle^p\ v\ \texttt{in}\ t \rhd^p x_{\{x:B\mid t\}}] \tag{10}$$
$$E[\texttt{true} \rhd^p v_{\{x:B\mid t\}}] \longrightarrow E[v_{\{x:B\mid t\}}] \tag{11}$$
$$E[\texttt{false} \rhd^p v_{\{x:B\mid t\}}] \longrightarrow \Uparrow p \tag{12}$$
$$E[\langle T \Leftarrow \{x : B \mid s\}\rangle^p\ v_{\{x:B\mid s\}}] \longrightarrow E[\langle T \Leftarrow B\rangle^p\ v] \tag{13}$$

Fig. 4. Run-time types and reduction

The type rules for variables, constants, lambda abstraction, and application are standard. The type rule for casts is straightforward: if term s has type S and type S is compatible with type T (defined below), then the term $\langle T \Leftarrow S\rangle^p\ s$ has type T.

We write $S \sim T$ for the *compatibility* relation, which holds if it may be sensible to cast type S to type T. A base type is compatible with itself, type $\texttt{Dyn}$ is compatible with any type, two function types are compatible if their domains and ranges are compatible, and a subset type is compatible with every type that is compatible with its domain.

Compatibility is reflexive and symmetric but not transitive. For example, $S \sim \texttt{Dyn}$ and $\texttt{Dyn} \sim T$ hold for any types S and T, but $S \sim T$ does not hold if one of S or T is a function type and the other is a base type. Requiring compatibility ensures that there

are no obviously foolish casts, but does not rule out the possibility of two successive casts, one from S to $\texttt{Dyn}$ and the next from $\texttt{Dyn}$ to T.

Our cast rule is inspired by the similar rules found for gradual types and hybrid types. Gradual types introduce compatibility, but do not have subset types. Hybrid types include subset types, but do not bother with compatibility. Neither system uses both positive and negative blame labels, as we do here.

Hybrid types also have a subsumption rule: if s has type S, and S is a subtype of T, then s also has type T. This greatly increases the power of the type system. For instance, in hybrid types each constant is assigned the singleton type $c : \{x : B \mid c = x\}$; and by subtyping and subsumption it follows that each constant belongs to every subset type $\{x : B \mid t\}$ for which $t[x := c] \longrightarrow^* \texttt{true}$. However, the price paid for this is that type checking for hybrid types is undecidable, because the subtype relation is undecidable.

A pleasant consequence of omitting subsumption from the blame calculus is that each term has a unique type, and an even more pleasant consequence is that the type system for the source language is decidable.

Proposition 1. *(Unicity) If $\Gamma \vdash s : S$ and $\Gamma \vdash s : T$ then $S = T$.*

Proposition 2. *(Decidability) Given Γ and t, it is decidable whether there is a T such that $\Gamma \vdash t : T$ (using the compile-time type rules of Figure 3).*

Both propositions are easy inductions.

However, there are some less pleasant consequences. (The tiger is caged, not tamed!) Reduction may introduce terms that are not permitted in the source language, and we need additional semidecidable run-time rules to check the types of these terms. We explain the details of how this works below.

3.2 Reductions

Figure 4 defines additional term forms, values, evaluation contexts, additional run-time type rules, and reduction.

We let v, w range over values. A value is either a variable, a constant, a lambda term, a cast to a function type from another function type, an injection into dynamic from a ground type, or an injection into a subset type from its domain type. The first three of these are standard, and we explain the other three below.

We take a cast to a function type from another function type as a value for technical convenience. Other work [15, 5] makes the opposite choice, and reduce a cast to a function type from another function type to a lambda expression.

Values of dynamic type take the form $\texttt{Dyn}_G(v)$, where G is ground type, which is either a base type B or the function type $\texttt{Dyn} \to \texttt{Dyn}$, and v is a value of type G. For example, the cast $\langle \texttt{Dyn} \Leftarrow \texttt{Int} \to \texttt{Int} \rangle^p\ (\lambda x : \texttt{Int}.\ x + 1)$ reduces to the value $\texttt{Dyn}_{\texttt{Dyn}\to\texttt{Dyn}}(\langle \texttt{Dyn} \to \texttt{Dyn} \Leftarrow \texttt{Int} \to \texttt{Int} \rangle^p\ (\lambda x : \texttt{Int}.\ x + 1))$. Note that the inner cast is a value, since it is to a function type from another function type.

Values of subset type take the form $v_{\{x:B|t\}}$ where v is a value of type B and $t[x := v] \longrightarrow^* \texttt{true}$. We also need an intermediate term to test the predicate associated with a cast to a subset type. This term has the form $s \rhd^p v_{\{x:B|t\}}$, where v is a value of type T, and s is a boolean term such that $t[x := v] \longrightarrow^* s$. If s reduces to $\texttt{true}$ the term reduces to $v_{\{x:B|t\}}$, and if s reduces to $\texttt{false}$ the term allocates blame to p.

(In contrast, Flanagan [5] has essentially the following rule.

$$\frac{t[x := v] \longrightarrow^* \texttt{true}}{\langle \{x : B \mid t\} \Leftarrow B \rangle^p \, v \longrightarrow v_{\{x:B|t\}}}$$

This formulation is unusual, in that a single reduction step in the conclusion depends on multiple steps in the hypothesis. The rule makes it awkward to formulate a traditional progress theorem, because if reduction of $t[x := v]$ proceeds forever, then evaluation gets stuck.)

We let E range over evaluation contexts, which are standard. The cast operation is strict, and reduces the term being cast to a value before the cast is performed, and the subset test is strict in its predicate.

We write $s \longrightarrow r$ to indicate that a single reduction step takes term s to result r, which is either a term t or the form $\Uparrow p$, which indicates allocation of blame to label p. We write $s \longrightarrow^* r$ for the reflexive and transitive closure of reduction.

There are three additional type rules for the three additional term forms. These are straightforward, save that the two rules for subset types involve reduction, and hence are semi-decidable. Hence, Proposition 2 (Decidability) holds only for the compile-time syntax type rules of Figure 3, and fails when these are extended with the run-time type rules of Figure 4. However, it is easy to check that Proposition 1 (Unicity), holds even when the compile-time type rules are extended with the run-time type rules.

The good news is that semi-decidability is not a show stopper. We introduce the semi-decidable type rules precisely in order to prove preservation and progress. Typing of the source language is decidable, and reduction is decidable. We never need to check whether a term satisfies the semi-decidable rules, since this is guaranteed by preservation and progress!

We now go through each of the reductions in turn. (1) Constants of function type are interpreted by a semantic function consistent with their type: if $\text{ty}(c) = S \to T$ and value v has type S, then $[\![c]\!](v)$ is a term of type T. For example, $\text{ty}(+) = \texttt{Int} \to \texttt{Int} \to \texttt{Int}$, with $[\![+]\!](3) = +_3$, where $\text{ty}(+_3) = \texttt{Int} \to \texttt{Int}$ and $[\![+_3]\!](4) = 7$. (2) The rule for applying a lambda expression is standard. (3) A cast to a base type from itself is the identity. (4) A cast to a function type from another function type decomposes into separate casts on the argument and result. Note the reversal in the argument cast, and the corresponding negating of the blame label.

The next three rules concern casts to the dynamic type. (5) A cast to `Dyn` from itself is the identity. (6) A cast to `Dyn` from a base type is a value. (7) A cast to `Dyn` from a function type $S \to T$ decomposes into a cast to `Dyn` from the ground type $\texttt{Dyn} \to \texttt{Dyn}$, and a cast to $\texttt{Dyn} \to \texttt{Dyn}$ from $S \to T$.

The next two rules concern casts from the dynamic type. (8) A cast to type T from the value $\texttt{Dyn}_G(v)$ of dynamic type collapses to a cast to type T directly from type G if the types T and G are compatible. (9) Otherwise, such a cast fails.

The next three rules concern casts to subset type. (10) A cast to subset type with domain B from type S decomposes into a cast to B from S, followed by a test that the value satisfies the predicate. (11) If the predicate evaluates to true the test reduces to the subset type. (12) Otherwise the test fails.

Entailment $\boxed{x : T \Leftarrow S \models t}$

$$\frac{S \sim T \qquad \text{for all } v \text{ and } w, \text{ if } \vdash v : S \text{ and } \langle T \Leftarrow S \rangle^p\ v \longrightarrow^* w \text{ then } t[x := w] \longrightarrow^* \texttt{true}}{x : T \Leftarrow S \models t}$$

Subtype $\boxed{S <: T}$

$$B <: B \qquad \texttt{Dyn} <: \texttt{Dyn}$$

$$\frac{S' <: S \qquad T <: T'}{S \to T <: S' \to T'} \qquad \frac{B <: T}{\{x : B \mid s\} <: T} \qquad \frac{S <: B \qquad x : B \Leftarrow S \models t}{S <: \{x : B \mid t\}} \qquad \frac{S <: G}{S <: \texttt{Dyn}}$$

Positive subtype $\boxed{S <:^+ T}$

$$B <:^+ B \qquad S <:^+ \texttt{Dyn}$$

$$\frac{S' <:^- S \qquad T <:^+ T'}{S \to T <:^+ S' \to T'} \qquad \frac{B <:^+ T}{\{x : B \mid s\} <:^+ T} \qquad \frac{S <:^+ B \qquad x : B \Leftarrow S \models t}{S <:^+ \{x : B \mid t\}}$$

Negative subtype $\boxed{S <:^- T}$

$$B <:^- B \qquad \texttt{Dyn} <:^- T$$

$$\frac{S' <:^+ S \qquad T <:^- T'}{S \to T <:^- S' \to T'} \qquad \frac{B <:^- T}{\{x : B \mid s\} <:^- T} \qquad \frac{S <:^- B}{S <:^- \{x : B \mid t\}} \qquad \frac{S <:^- G}{S <:^- T}$$

Naive subtype $\boxed{S <:_n T}$

$$B <:_n B \qquad S <:_n \texttt{Dyn}$$

$$\frac{S <:_n S' \qquad T <:_n T'}{S \to T <:_n S' \to T'} \qquad \frac{B <:_n T}{\{x : B \mid s\} <:_n T} \qquad \frac{S <:_n B \qquad x : B \Leftarrow S \models t}{S <:_n \{x : B \mid t\}}$$

Fig. 5. Subtypes

The last rule concerns casts from a subset type. (13) Consider a cast to type T from a subset type. Recall that values of subset type have the form $v_{\{x:B|s\}}$, where v has type B. The cast collapses to a cast directly to T from B. Note that B and T must be compatible, since a subset type is only compatible with a type that is compatible with its domain.

3.3 Subtyping

We do not need subtyping to assign types to terms, but we will use subtyping to characterise when a cast cannot give rise to blame. Figure 5 presents entailment and four subtyping judgements—ordinary, positive, negative, and naive.

Entailment is written

$$x : T \Leftarrow S \models t$$

and holds if for all values v of type S and w of type T such that $\langle T \Leftarrow S \rangle^p\ v \longrightarrow^* w$ we have that $t[x := w] \longrightarrow^* \texttt{true}$.

We write $S <: T$ if S is a subtype of T. Function subtyping is contravariant in the domain and covariant in the range. A subset type is a subtype of its domain, and a type is a subtype of a subset type if membership in the type entails satisfaction of the subset

type's predicate. Every subtype of a ground type is a subtype of $\texttt{Dyn}$, since casts from subtypes of a ground type to $\texttt{Dyn}$ cannot allocate blame.

For example, say that we define $\texttt{Pos} = \{x : \texttt{Int} \mid x > 0\}$ and $\texttt{Nat} = \{x : \texttt{Int} \mid x \geq 0\}$. Then $x : \texttt{Int} \Leftarrow \texttt{Pos} \models x \geq 0$, and so $\texttt{Pos} <: \texttt{Nat}$ by the sixth rule. For another example, $\texttt{Int} <: \texttt{Int}$ by the first rule, so $\texttt{Pos} <: \texttt{Int}$ by the fifth rule, so $\texttt{Pos} <: \texttt{Dyn}$ by the third rule.

Entailment, and hence subtyping, are undecidable. This is not a hindrance, since our type system does not depend on subtyping. Rather it is an advantage, since it means we can show more types are in the subtype relation, making our results more powerful.

Our rules for subtyping are similar to those found in earlier work [5, 8, 13]. However, they take every type to be a subtype of $\texttt{Dyn}$. In contrast, we only take S to be a subtype of T if a cast from S to T can never receive any blame, and therefore the only subtypes of $\texttt{Dyn}$ are $\texttt{Dyn}$ itself and subtypes of ground types. It is not appropriate to take function types (other that $\texttt{Dyn} \to \texttt{Dyn}$) as subtypes of $\texttt{Dyn}$, because a cast to $\texttt{Dyn}$ from a function type may receive negative blame. The issues are similar to the treatment of the contract $\texttt{Any}$ [3].

In order to characterize when positive and negative blame cannot occur, we factor subtyping into two subsidiary relations, positive subtyping, written $S <:^+ T$ and negative subtyping, written $S <:^- T$. The two judgements are defined in terms of each other, and track the swapping of positive and negative blame labels that occurs with function types, with the contravariant position in the function typing rule reversing the roles. We have $S <:^+ \texttt{Dyn}$ and $\texttt{Dyn} <:^- T$ for every type S and T, since casting to $\texttt{Dyn}$ can never give rise to positive blame, and casting from $\texttt{Dyn}$ can never give rise to negative blame. We only check entailment between subtypes for positive subtyping, since failure of a subset predicate gives rise to positive blame. Finally, on the negative side, if $S <:^- G$, then $S <:^- T$, since no cast from a subtype of a ground type to any other type can allocate negative blame.

Proposition 3. *(Subtyping is transitive and reflexive) If $S <: S'$ and $S' <: S''$ then $S <: S''$, for all S, S', S'', and $S <: S$, for all S. Similarly for $<:^+$, $<:^-$, and $<:_n$.*

Proposition 4. *(Subtyping and compatibility) If $S <: T$ then $S \sim T$. Similarly for $<:^+$ and $<:_n$, but not $<:^-$.*

The main results concerning positive and negative subtyping are given in Section 4. We show that $S <: T$ if and only if $S <:^+ T$ and $S <:^- T$. We also show that if $S <:^+ T$ then a cast from S to T cannot receive positive blame, and that if $S <:^- T$ then a cast from S to T cannot receive negative blame.

We also define a naive subtyping judgement, $S <:_n T$, which corresponds to our informal notion of type S being more precise than type T, and is covariant for both the domain and range of functions. In Section 4, we show that $S <:_n T$ if and only if $S <:^+ T$ and $T <:^- S$. (Note the reversal! In the similar statement for ordinary subtyping, we wrote $S <:^- T$, where here we write $T <:^- S$.)

Here are some examples:

$$\texttt{Int} \to \texttt{Nat} <: \texttt{Nat} \to \texttt{Int} \qquad \texttt{Nat} \to \texttt{Nat} <:_n \texttt{Int} \to \texttt{Int}$$
$$\texttt{Int} \to \texttt{Nat} <:^+ \texttt{Nat} \to \texttt{Int} \qquad \texttt{Nat} \to \texttt{Nat} <:^+ \texttt{Int} \to \texttt{Int}$$
$$\texttt{Int} \to \texttt{Nat} <:^- \texttt{Nat} \to \texttt{Int} \qquad \texttt{Int} \to \texttt{Int} <:^- \texttt{Nat} \to \texttt{Nat}$$

Syntax

untyped terms $\quad M, N ::= x \mid k \mid \lambda x.\ N \mid M\ N \mid \lfloor t \rfloor$

Well-formed terms $\boxed{\Gamma \vdash M \text{ wf}}$

$$\frac{(x : \texttt{Dyn}) \in \Gamma}{\Gamma \vdash x \text{ wf}} \qquad \frac{\Gamma,\, x : \texttt{Dyn} \vdash N \text{ wf}}{\Gamma \vdash (\lambda x.\ N) \text{ wf}} \qquad \frac{\Gamma \vdash M \text{ wf} \qquad \Gamma \vdash N \text{ wf}}{\Gamma \vdash (M\ N) \text{ wf}} \qquad \frac{\Gamma \vdash t : \texttt{Dyn}}{\Gamma \vdash \lfloor t \rfloor \text{ wf}}$$

Embedding $\boxed{\lceil M \rceil}$

$$\begin{array}{ll} \lceil x \rceil & = x \\ \lceil c \rceil & = \langle \texttt{Dyn} \Leftarrow \mathsf{ty}(c) \rangle\ c \\ \lceil \lambda x.\ N \rceil & = \langle \texttt{Dyn} \Leftarrow \texttt{Dyn} \to \texttt{Dyn} \rangle\ (\lambda x : \texttt{Dyn}.\ \lceil N \rceil) \\ \lceil M\ N \rceil & = (\langle \texttt{Dyn} \to \texttt{Dyn} \Leftarrow \texttt{Dyn} \rangle\ \lceil M \rceil)\ \lceil N \rceil \\ \lceil \lfloor t \rfloor \rceil & = t \end{array}$$

Fig. 6. Untyped lambda calculus

The left-hand side line shows that ordinary subtyping is contravariant in the domain and covariant in the range, while the right-hand side shows that naive subtyping is covariant in both. In both cases, the first line is equivalent to the second and third.

3.4 Typed and untyped lambda calculus

We introduce a separate grammar for untyped terms, and show how to embed untyped terms into typed terms (and vice versa). The relevant definitions are in Figure 6.

Let M, N range over untyped terms. The term form $\lfloor t \rfloor$ lets us embed typed terms into untyped terms; it is well-formed only if the typed term t has type `Dyn`. Below we define a mapping $\lceil M \rceil$, that lets us embed untyped terms into typed terms.

An untyped term is well-formed if every variable appearing free in it has type `Dyn`, and if every typed subterm has type `Dyn`. We write $\Gamma \vdash M$ wf to indicate that M is well-formed.

A simple mapping takes untyped terms into typed terms. An untyped term M is well-formed if and only if the corresponding typed term $\lceil M \rceil$ is well-typed with type `Dyn`.

Lemma 1. *We have $\Gamma \vdash M$ wf if and only if $\Gamma \vdash \lceil M \rceil : \texttt{Dyn}$.*

It is straightforward to define reduction for untyped terms, and show that the embedding preserves and reflects reductions.

3.5 Type safety

We have usual substitution and canonical forms lemmas, and preservation and progress results.

Lemma 2. *(Substitution) If $\Gamma \vdash v : S$ and $\Gamma,\, x : S \vdash t : T$, then $\Gamma \vdash t[x := v] : T$.*

Lemma 3. *(Canonical forms) Let v be a value that is well-typed in the empty context. One of three cases applies.*

- *If $\vdash v : S \to T$ then either*
  - *$v = \lambda x : S.\ t$, with $x : S \vdash t : T$, or*

$$\frac{S <:^{+} T \qquad s \text{ safe for } p}{\langle T \Leftarrow S\rangle^{p} s \text{ safe for } p} \qquad \frac{S <:^{-} T \qquad s \text{ safe for } p}{\langle T \Leftarrow S\rangle^{\bar{p}} s \text{ safe for } p} \qquad \frac{p \neq q \qquad \bar{p} \neq q \qquad s \text{ safe for } p}{\langle T \Leftarrow S\rangle^{q} s \text{ safe for } p}$$

$$\frac{v \text{ safe for } p}{\mathtt{Dyn}_{G}(v) \text{ safe for } p} \qquad \frac{s \longrightarrow^{*} \mathtt{true}}{s \rhd^{p} v_{\{x:B|t\}} \text{ safe for } p} \qquad \frac{q \neq p \qquad s \text{ safe for } p}{s \rhd^{q} v_{\{x:B|t\}} \text{ safe for } p}$$

$$\frac{}{x \text{ safe for } p} \qquad \frac{}{c \text{ safe for } p} \qquad \frac{t \text{ safe for } p}{\lambda x : S.\ t \text{ safe for } p} \qquad \frac{t \text{ safe for } p \qquad s \text{ safe for } p}{t\ s \text{ safe for } p}$$

Fig. 7. Safe terms

- $v = c$, *with* $\mathrm{ty}(c) = S \to T$, *or*
- $v = \langle S \to T \Leftarrow S' \to T'\rangle^{p}\ v'$ *with* $\vdash v' : S' \to T'$.

– *If* $\vdash v : \{x : B \mid t\}$ *then* $v = v'_{\{x:B|t\}}$ *with* $\vdash v' : B$ *and* $t[x := v'] \longrightarrow^{*} \mathtt{true}$.
– *If* $\vdash v : \mathtt{Dyn}$ *then* $v = \mathtt{Dyn}_{G}(v')$ *with* $\vdash v' : G$.

Proposition 5. *(Preservation) If* $\Gamma \vdash s : T$ *and* $s \longrightarrow t$ *then* $\Gamma \vdash t : T$.

Proposition 6. *(Progress) If* $\vdash s : T$ *then either*

– s *is a value, or*
– $s \longrightarrow t$ *for some result* t*, or*
– $s \longrightarrow \Uparrow p$ *for some blame label* p.

In this case, preservation and progress do not guarantee a great deal, since they do not rule out blame as a result. However, Section 4 gives results that let us identify circumstances where certain kinds of blame cannot arise.

4 The blame theorem

Subtyping factors into positive and negative subtyping, and naive subtyping also factors into positive and negative subtyping, this time with the direction of negative subtyping reversed.

Proposition 7. *(Factoring subtyping) We have* $S <: T$ *if and only if* $S <:^{+} T$ *and* $S <:^{-} T$.

Proposition 8. *(Factoring naive subtyping) We have* $S <:_{n} T$ *if and only if* $S <:^{+} T$ *and* $T <:^{-} S$.

The following is the central result of this paper and depends on the definition of the safe for relation. A term t is safe for a blame label p if all of the casts that have the label p are positive subtypes, all of the casts that have the label $\neg p$, are negative subtypes, and all of the predicate tests with the label p succeed. The precise definition is given in Figure 7.

Proposition 9. *(Preservation of safe terms) For any well-typed term* t *and blame label* p*, if* t safe for p *and* $t \longrightarrow t'$ *then* t' safe for p.

Proposition 10. *(Progress of safe terms) For any well-typed term t and blame label p, if t* safe for p *then $t \not\longrightarrow \Uparrow p$.*

Corollary 1. *(Well-typed programs can't be blamed) Let t be a well-typed term with a subterm $\langle T \Leftarrow S \rangle^p\ s$ containing the only occurrences of p in t.*

- *If $S <:^+ T$ then $t \not\longrightarrow^* \Uparrow p$.*
- *If $S <:^- T$ then $t \not\longrightarrow^* \Uparrow \bar{p}$.*
- *If $S <: T$ then $t \not\longrightarrow^* \Uparrow p$ and $t \not\longrightarrow^* \Uparrow \bar{p}$*

In particular, since $S <:^+ \texttt{Dyn}$, any failure of a cast from a well-typed term to a dynamically-typed context must be blamed on the dynamically-typed context. And since $\texttt{Dyn} <:^- T$, any failure of a cast from a dynamically-typed term to a well-typed context must be blamed on the dynamically-typed term.

Further, consider a cast from a more precise type to a less precise type, which we can capture using naive subtyping. Since $S <:_n T$ implies $S <:^+ T$, any failure of a cast from a more-precisely-typed term to a less-precisely-typed context must be blamed on the less-precisely-typed context. And since $T <:_n S$ implies $S <:^- T$, any failure of a cast from a less-precisely-typed term to a more-precisely-typed context must be blamed on the less-precisely-typed term.

5 Related work

Integrating static and dynamic typing is not new, and previous work includes type Dynamic [1], soft types [21], and partial types [16]. Contracts for dynamic testing of specifications were popularized by the language Eiffel [12]. Findler and Felleisen [4] introduced the use of higher-order contracts with blame in functional programming.

Henglein [9] lays much of the theoretical ground work for combining typed and untyped program fragments in a single program. Our work's principal technical debt concerns canonical coercions and the results surrounding them which justify our writing of casts as just a pair of types, instead of a pair of types combined with an explicit coercion (as Henglein does). Due to a coincidence of terminology, it is natural to compare Henglein's positive and negative coercions with our positive and negative subtyping relations, but they are essentially unrelated. Henglein's positive and negative coercions simply characterize naive subtyping [9, Proposition 23].

Siek and Taha [15] introduced gradual types, inspired by Gray et al [6]. Our results augment theirs, since we show how the blame for a failed cast always lies with the less-typed portion of the code. Siek, Garcia, and Taha [14] compare various approaches to subtyping for gradual types, including the one considered in this paper.

Flanagan et al [5, 8] introduced hybrid types and a new programming language, Sage. Ou et al [13] present a closely-related language with dynamically-checked dependent types. These support dependent function types, while our work here is restricted to ordinary function types.

Acknowledgements. This paper benefited enormously from conversations with John Hughes. Thanks to Samuel Bronson, Matthias Felleisen, Cormac Flanagan, Oleg Kiselyov, Jeremy Siek, and anonymous referees of earlier drafts for their comments on the paper. A special thanks to Michael Greenberg, Nate Foster, and Benjamin Pierce for discovering a technical flaw in an earlier version.

References

[1] Abadi, M., L. Cardelli, B. Pierce and G. Plotkin. Dynamic typing in a statically typed language. *ACM Trans. Prog. Lang. Syst.*, 13(2):237–268, April 1991.

[2] Bracha, G. Pluggable type systems. In *OOPSLA'04 Workshop on Revival of Dynamic Languages*, October 2004.

[3] Findler, R. and M. Blume. Contracts as pairs of projections. In *International Symposium on Functional and Logic Programming (FLOPS)*, April 2006.

[4] Findler, R. B. and M. Felleisen. Contracts for higher-order functions. In *ACM International Conference on Functional Programming (ICFP)*, October 2002.

[5] Flanagan, C. Hybrid type checking. In *ACM Symposium on Principles of Programming Languages (POPL)*, Janurary 2006.

[6] Gray, K. E., R. B. Findler and M. Flatt. Fine-grained interoperability through contracts and mirrors. In *ACM Conference on Object-Oriented Programming: Systems, Languages, and Applications (OOPSLA)*, pages 231–246, 2005.

[7] Gronski, J. and C. Flanagan. Unifying hybrid types and contracts. In *Trends in Functional Programming (TFP)*, April 2007.

[8] Gronski, J., K. Knowles, A. Tomb, S. N. Freund and C. Flanagan. Sage: Hybrid checking for flexible specifications. In *Workshop on Scheme and Functional Programming*, September 2006.

[9] Henglein, F. Dynamic typing: Syntax and proof theory. *Sci. Comput. Programming*, 22(3):197–230, 1994.

[10] Matthews, J. and R. B. Findler. Operational semantics for multi-language programs. In *ACM Symposium on Principles of Programming Languages (POPL)*, Janurary 2007.

[11] Meijer, E. Static typing where possible, dynamic typing where needed. In *OOPSLA'04 Workshop on Revival of Dynamic Languages*, October 2004.

[12] Meyer, B. *Object-Oriented Software Construction*. Prentice Hall, 1988.

[13] Ou, X., G. Tan, Y. Mandelbaum and D. Walker. Dynamic typing with dependent types. In *IFIP International Conference on Theoretical Computer Science*, August 2004.

[14] Siek, J., R. Garcia and W. Taha. Exploring the design space of higher-order casts. In *European Symposium on Programming (ESOP)*, 2009.

[15] Siek, J. G. and W. Taha. Gradual typing for functional languages. In *Workshop on Scheme and Functional Programming*, September 2006.

[16] Thatte, S. Type inference with partial types. In *International Colloquium on Automata, Languages and Programming*, volume 317 of *LNCS*. Springer-Verlag, 1988.

[17] Tobin-Hochstadt, S. and M. Felleisen. Interlanguage migration: From scripts to programs. In *Dynamic Languages Symposium (DLS)*, 2006.

[18] Tobin-Hochstadt, S. and M. Felleisen. The design and implementation of typed scheme. In *ACM Symposium on Principles of Programming Languages (POPL)*, 2008.

[19] Wadler, P. and R. B. Findler. Well-typed programs can't be blamed. In *Workshop on Scheme and Functional Programming*, September 2007.

[20] Wadler, P. and R. B. Findler. Well-typed programs can't be blamed. Technical Report TR-2009-01, University of Chicago, 2009.

[21] Wright, A. K. and R. Cartwright. A practical soft typing system for Scheme. *ACM Trans. Prog. Lang. Syst.*, 19(1), 1997.

A Appendix

This appendix contains the proofs omitted from the main body of the paper.

A.1 Proof of the typing results, lemmas 2 and 3, propositions 5 and 6

*** Lemma G+x:S |- t:T and x not in the free vars of t implies G |- t:T**

By induction.

*** Substitution: G |- v:S and G+x:S |- t:T implies G |- t[x:=v] : T.**

Proof by induction on the structure of the derivation that x:S|-t:T.

**** t = y**

If x=y then from S=T and t[x:=v] = v and thus G |- [x:=v]:T.
If x=/=y then t[x:=v] = t and since x is not free in t, we can
narrow G, and thus G |- t : T.

**** t = c**

x is not free in t, follows from the lemma above.

**** t = \x':S'.t'**

In this case, T must be S'->S'' and the last step in the derivation
must have been:

```
G + x:S + x':S' |- t' : S''
-------------------------------[lam]
G + x:S |- \x':S'.t' : S' -> S''
```

If x'=x, then x does not appear free in t' and the lemma above gives
us the result. If x =/= x', then we know by induction that

G + x':S' |- t'[x:=v] : S''

and we can reapply the function rule to conclude that G |- t[x:=v] : T.

**** t = s' s''**

By induction.

**** t = <S' = T'> s'**

By induction.

**** t = Dyn_G(s')**

By induction.

**** t = v'_{x':B|s'}**

In this case, T must be {x:B|s'} and the last step in the derivation that G+x:S |- t:T must have been:

```
 G + x:S |- v' : B     s'[x':=v'] -->* true
-----------------------------------------
     G + x:S |- v'_{x':B|s'} : {x':B|s'}
```

By induction, G |- v'[x:=v] : B.

Also, we know that s'[x':=v'][x:=v] = s'[x':=v'] because the only free variable in s' is x' since {x':B|s'} is a well-formed type. Thus we can conclude that G |- t[x:=v] : T

**** t = s' |>p v'_{x':B|u'}**

In this case, T = {x':B|u'} and the last step in the derivation must have been

```
 G+x:S |- s' : bool
 G+x:S |- v'_{x':B|u} : {x':B|u}
 u'[x':=v'] -->* s'
-----------------------------------------
 G+x:S |- s' |>p v'_{x':B|u'} : {x':B|u'}
```

From induction, we know that

```
 G |- s'[x:=v] : bool
 G |- v'_{x':B|u}[x:=v] : {x':B|u}
```

Also, we know that s'[x':=v'][x:=v] = s'[x':=v'] because the only free variable in s' is x' since {x':B|s'} is a well-formed type. Thus we can conclude that G |- t[x:=v] : T

*** Canonical forms**

If |- v : S -> T then either:

```
  v = \x:S.t with x:S |- t:T
  v = c with ty(c) = S -> T, or
  v = <S->T <= S'->T'>p v' with |- v' : S' -> T'
```

If |- v : {x:B|t} then

```
  v = v'_{x:B|t} and |- v' : B and t[x:=v'] ->* true
```

If |- v : Dyn then

```
  v = Dyn_G(v') and |- v' : G
```

Follows by a simple case analysis (noting that c cannot have either the type Dyn or the type {x:B|t} for any x, B, or t).

*** Lemma: if E[t] : S then there is a T s.t. t:T and for all t':T, E[t'] : S.**

By induction on the structure of E.

*** Preservation: if G |- s:T and s --> t then G |- t:T**

By cases on the reduction sequence. We apply the lemma just above in every case, but without mentioning it. In many situations the type environment does not change, so we just omit it from the judgments written below.

**** E[c v] --> E[[[c]] v]**

**** E[(\x:T.s) v] --> E[s[x:=v]]**

By the substitution lemma.

**** E[<B <= B>p v] --> E[v]**

The right-hand side is a sub-derivation of the left.

**** E[(<S'->T' <= S->T>p v) w] --> E[<T'<=T>p (v (<S<=S'>p w))]**

From the left-hand side, we have this derivation:

```
    v : S -> T    S'->T' ~ S->T
--------------------------------[cast]
(<S'->T' <= S->T>p v) : S'->T'         w : S'
-----------------------------------------------[app]
 (<S'->T' <= S->T>p v) w : T'
```

From the definition of ~, we knopw that S'->T' ~ S->T means that S'~S and T'~T. Furthermore, ~ is symmetric, so S~S'

Then using the casting typing rule, the application rule, the derivations of v : S -> T and w : S', and the fact that S->T~S'->T' we can build this derivation for the right-hand side:

```
                w : S'   S~S'
             ----------------
 v : S -> T   <S<=S'>p w
---------------------------[app]
  (v (<S<=S'>p w)) : T   T'~T
-----------------------------[cast]
<T'<=T> (v (<S<=S'>p w)) : T'
```

**** E[<Dyn<=Dyn>p v] --> E[v]**

The right-hand side is a sub-derivation of the left-hand side.

**** E[<Dyn<=B>p v] --> E[Dyn_B(v)]**

From the left we have this derivation:

```
   v : B      Dyn ~ B
-----------------------[cast]
 <Dyn <= B> p v : Dyn
```

And using the derivation that v : B, we can construct one for the right:

```
   v : B
-------------[Dyn]
Dyn_B(v) : B
```

**** E[<Dyn<=S->T>p v] --> E[Dyn_{Dyn->Dyn} (<Dyn->Dyn <= S->T>p v)]**

From the left we have this derivation:

```
    v : S -> T   Dyn ~ S->T
------------------------------[cast]
     <Dyn<=S->T>p v : Dyn
```

which lets us construct this one for the right (since Dyn->Dyn ~ S->T for any S and T).

```
       v : S -> T        Dyn->Dyn ~ S->T
-------------------------------------------[cast]
    <Dyn->Dyn <= S->T> v : Dyn->Dyn
-------------------------------------------[Dyn]
Dyn_{Dyn->Dyn} (<Dyn->Dyn <= S->T> v) : Dyn
```

**** E[<T <= Dyn>p Dyn_G(v)] --> E[<T <= G>p v] if G ~ T**

Given:

```
         v : G
  -----------------[Dyn]
    Dyn_G(v) : Dyn    Dyn ~ T
------------------------------[cast]
  <T <= Dyn>p Dyn_G(v) : T
```

So we can build this one:

```
 v : G          G ~ T
-----------------------[cast]
   <T <= G>p v : T
```

**** E[<T <= Dyn>p Dyn_G(v)] --> blame(p) if T ~/~ G**

Vacuously true.

**** E[<{x:B|t} <= S>p v] --> E[let x=<B<=S>p v in t |>p x_{x:B|t}]**

Given:

```
  G |- v : S       S ~ {x:B|t}
-----------------------------------[cast]
G |- <{x:B|t} <= S>p v : {x:B|t}
```

To build the derivation for the right hand side, we need:

- the sub-derivation G |- v:S above
- S ~ B, which we get from S ~ {x:B|t}
- t[x:=x] -->* t (filling in the variables from the rule),
  which trivially holds.

Also, we treat the let expression as a shorthand for an immediately
applied lambda expression with, in this case, a parameter of type B.

```
by assumption
that all types
are well-formed
----------------[wf]  --------------[var]
G+{x:B} |- t : B      G+{x:B} |- x:B      t[x:=x] -->* t     G |- v:S      S ~ B
-------------------------------------------------------[|>] -------------------[cast]
       G+{x:B} |- t |>p x_{x:B|t} : {x:B|t}                 G |- <B<=S>p v : B
-------------------------------------------------------------------------------------[let]
               G |= let x=<B<=S>p v in t |>p x_{x:B|t} : {x:B|t}
```

**** E[true |>p v_{x:B|t}] --> E[v_{x:B|t}]**

From the left-hand side, we get this:

```
-----------[T]
true : Bool     v : B    t[x:=v] -->* true
-------------------------------------------[|>]
true |>p v_{x:B|t} : {x:B|t}
```

which gives us the subderivations to construct this tree:

```
v : B    t[x:=v] -->* true
---------------------------[sub]
v_{x:B|t} : {x:B|t}
```

**** E[false |>p v_{x:B|t}] --> blame(p)**

Vacuously true.

**** E[<T <= {x:B|s}>p v_{x:B|s}] --> E[<T <= B>p v]**

From the left-hand side we get this:

```
v : B    s[x:=v] -->* true
---------------------------[sub]
   v_{x:B|s} : {x:B|s}              {x:B|s} ~ T
-------------------------------------------------[cast]
      <T <= {x:B|s}>p v_{x:B|s} : {x:B|s}
```

{x:B|s} ~ T tell us that B ~ T and we can use the derivation that v:B
to build this derivation for the right-hand side.

```
 v : B   B ~ T
----------------[cast]
<T <= B>p v : T
```

***** Progress: if |- s : T then s -> t, s -> blame(p) or s is a value.**

By induction on the structure of s.

**** s = x**

Does not typecheck.

**** s = c**

Is a value

**** s = \x:S.s'**

Is a value.

**** s = t' s'**

If either t' or s' are not values, then by induction plus the
definition of evaluation contexts, we know that s reduces.

Since s : T, by inversion we know that t' : S' -> T and s' : S'.
By canonical forms, then, there are three possibilities for t'

***** t' = \x:S.t**

In this case, t' s' reduces by rule (2).

***** t' = c with ty(c) = S->T**

In this case, s reduces as the constant c dictates.

***** t' = <S->T <= S'->T'>p v'**

In this case, rule (4) applies and thus t' reduces.

**** s = <T <= S>p s'**

If s' reduces, then s reduces, since the evaluation contexts include <T <= S>p E. If s' does not reduce, then it must be a value, v.

Consider T's structure:

***** T = Dyn**

Consider S's structure. If S = Dyn, the expression reduces by (5). If S = B, then s reduces by (6). If S = S'->S'' then t reduces by (7). If S = {x:B|t}, then the typing judgments tell us that v has type {x:B|t}, and the canonical forms lemma tells us that v = v'_{x:B|t}. Thus, t reduces by (13).

***** T = B**

Consider S's structure. If S = Dyn, then canonical forms tells us that v = Dyn_G(v'), and either (8) or (9) applies, depending if G ~ T or not. If S = B, then s reduces by (3). S cannot be S' -> S'' because B ~/~ S' -> S'' and the typing rules insist that S~T. If S={x:B|t}, canonical forms and the typing rules again tell us that v=v'_{x:B|t}, and thus s reduces by (13).

***** T = T' -> T''**

Consider S's structure. If S = Dyn, then canonical forms tells us that v = Dyn_G(v') and either (8) or (9) applies, depending if G ~ T or not. S cannot be B or {x:B|s'|, since the typing rules insist that S~T. If S is S'->S'', then <T<=S> v is also a value.

***** T = {x:B|t}**

Rule (10) applies.

**** s = Dyn_G(v)**

This is a value.

**** s = v_{x:B|t'}**

This is a value.

**** s = s' |>p v_{x:B|t}**

If s' reduces, then so does s. Thus, by induction we can assume that s' = v'. Since the typing rules tell us that s' : Bool, then we know that s is either true (so rule (11) applies) or false (so rule (12) does).

A.2 Proof that the subtyping relations are transitive, proposition 3

*** Transitivity for <: and <:n**

Follows from the factoring lemmas and the transitivity arguments below.

*** Transitivity for <:+. S <:+ R and R <:+ T implies S <:+ T**

Cases are ordered by the order in which the rules appear in main body of the paper. I just skipped cases where the relevant rules cannot apply due to structural mismatches and I didn't write out the cases where T is Dyn, or where two of the S, R, and T are identical (ie, both a specific B).

**** case 1. S <:+ R by first rule. Thus S = R = B**
***** case 1a. R <:+ T by rule 1. Thus T = B.**
***** case 1b. R <:+ T by rule 2. Thus T = Dyn.**
***** case 1c. R <:+ T by rule 5. Thus T = {x:B|t}.**
Follows immediately because S = R and R <:+ T.

**** case 2. S <:+ R by second rule. Thus, R = Dyn.**
***** case 2a, R <:+ T by rule 2. Thus T = Dyn.**
***** case 2b, R <:+ T by rule 5. Thus T = {x:B|t} and Dyn <:+ B.**

This cannot happen, since Dyn <:+ B is not derivable.

**** case 3. S <:+ R by the third rule. Thus S=S'->S'' and R=R'->R''.**
***** case 3a. R <:+ T by rule 2. Thus T = Dyn.**
***** case 3b. R <:+ T by rule 3. Thus T = T'->T''.**
Follows from induction.
***** case 3c. R <:+ T by rule 5. Thus T = {x:B|t}. and R <:+ B.**
Cannot happen, since R'->R'' <:+ B is not derivable.

**** case 4. S <:+ R by the fourth rule. Thus S={x:B|t} and B <:+ R.**
***** case 4a. R <:+ T by rule 1. Thus R=T=B.**
***** case 4b. R <:+ T by rule 2. Thus T=Dyn.**
***** case 4c. R <:+ T by rule 3. Thus R=R'->R'' and T=T'->T''**
This cannot happen, since B <:+ R'->R'' is not derivable.

***** case 4d. R <:+ T by rule 4. Thus R={x:B'|t'} and B' <:+ T.**
So, we know that B <:+ {x:B'|t'}. The only rule that can deduce that is the fifth rule, so we also know that B <:+ B'. Thus, by induction, B <:+ T. Reapplying the fourth rule, we have that S <:+ T.

***** case 4e. R <:+ T by rule 5. Thus T = {x:B'|t'}, R <:+ B', and x:B'<=R |= t'**

Since B <:+ R and R <:+ B', then B <:+ B'. Furthermore, the only way
to derive B <:+ B' is if B=B'.

Since R <:+ B, R = B or R = {x:B|s}. If R=B, then we have all of the
pieces for this derivation:

```
B <:+ B'    x:B<=B |= t'
--------------------------
B <:+ {x:B|t'}
----------------------
{x:B|t} <:+ {x:B|t'}
```

Assume R={x:B|s}. Our goal is still the above derivation, and we need
to show that x:B<=B |= t'. So, let v,w be given such that v:B and
<B<=B>v -->* w. This also tells us that v=w. We need to show that
t'[x:=v] -->* true.

The only way to derive B <:+ R is rule 5, which tells us that
x:B<=B |= s and thus for every v:B, we have s[x:=v] -->* true.

Consider <B<={x:B|s}><{x:B|s}<=B>v. This reduces to
<B<={x:B|s}>v_{x:B|s} (by reduction rule 10 and the fact that s[x:=v]
-->* true). By x:B<=R |= t' (from the assumption of case 4e), and the fact that
<B<={x:B|s}>v_{x:B|s} --> v, we know that t[x:=v] -->* true, thus establishing
that x:B<=B |= t', so we can use the above derivation again to show that
S <:+ T.

**** case 5. S <:+ R by fifth rule. Thus R = {x:B|t}, S <:+ B, and x: B <= S |= t**

***** case 5a. R <:+ T by rule 3. Thus T = Dyn.**
***** case 5b. R <:+ T by rule 4. Thus B <:+ T.**

Follows by induction that S <:+ T.

***** case 5c. R <:+ T by rule 5. Thus T={x:B'|t'}, R <:+ B', and x:B' <= R |= t'**

The goal is to use rule 5 to show that S <:+ T.

First we need S <:+ B'. So we split things up based on the derivation
that R <:+ B'.

   Using Rule 1. can't happen, since R =/= B.
   Using Rule 2. can't happen, since B =/= Dyn.
   Using Rule 3. can't happen, since R =/= R'->R''.
   Using Rule 4. Thus B <:+ B'. By induction we have S <:+ B' Also, B=B'
   Using Rule 5. can't happen, since U =/= {x:U''|t''}

Next we need to show that x:B<=S |= t'.

Let v,w be given such that <B<=S> v -->* w. Need t'[x:=w] -->* true.
By x:B<=S|=t, we know that t[x:=w] -->* true.

```
      <B <= {x:B|t}><{x:B|t}<=B>w
 -->* <B <= {x:B|t}>w_{x:B|t}       by rule 10 & above observation
 --> w                              by rule 13
```

Thus, we have satisfied the requirements to use x:B<={x:B|t} |= t'
to show that t'[x:=w] -->* true and thus x:B<=S |= t'.

*** Transitivity for <:-. S <:- R and R <:- T implies S <:- T**

**** case 1. S <:- R by the rule one. Thus S = R = B**
**** case 2. S <:- R by the rule two. Thus S = Dyn.**

Reapply case 2 to get Dyn <:- T.

**** case 3. S <:- R by rule three. Thus S = S'->S'' and R=R'->R''**

***** case 3a. R <:- T by rule three. Thus T=T'->T''.**

Follows by induction.

***** case 3b. R <:- T by rule five. Thus, T={x:B|t} and R <:- B**

The only rule that matches the pattern R'->R'' <:- B is rule 6. From
that we know that R'->R'' <:- G. From the case analysis in lemma in
the factoring section, we know that R must be Dyn -> Dyn.

Since S'->S'' <:- Dyn->Dyn and Dyn->Dyn = G, then we know that S'->S''
<: T by rule 6.

***** case 3c. R <:- T by rule 6. Thus R <:- G.**

This hold by the same reasoning as in case 3b.

**** case 4. S <:- R by rule four. Thus S = {x:B|s} and B <:- R.**

***** case 4a. R <:- T by rule one. Thus R=T=B.**
***** case 4b. R <:- T by rule five. Thus T={x:B'|t'} and R <:- B'**

By induction, we know that U <:- B'. Thus we can apply both rules four
and five to conclude that S <:- T.

***** case 4c. R <:- T by rule 6. Thus R <:- G.**

Since B <:- G, by rule 6 we have B <:- T and by rule 4, we have
S <:- T.

**** case 5. S <:- R by rule five. Thus, R = {x:B|t} and S <:- B**

Since S <:- G, we can use rule 6 to conclude that S <:- T.

**** case 6. S <:- R by rule 6. Thus S <:- G.**

By rule 6 again, we have S <:- T.

*** S <: S**

Proceeds by induction on the structure of S. If S=B or Dyn it is immediate, and if S=S'->S'', it follows from induction. The only interesting case is when S={x:B|t}. In that case, we use this derivation:

```
  B <: B
------------
{x:B|t} <: B    x:B<={x:B|t} |= t
---------------------------------
      {x:B|t} <: {x:B|t}
```

which boils down to showing x:B<={x:B|t} |= t. So, let a v, w be given such that |- v : {x:B|t} and <B <= {x:B|t}>v -->* w. By the canonical forms lemma, we know that v = v'_{x:B|t} and that t[x:=v'] -->* true. Thus, the reduction sequence above is

```
 <B <= {x:B|t}> v'_{x:B|t} --> <B <= B> v' --> v'.
```

Thus, we know that v' = w and we have x:B<={x:B|t} |= t.

*** S <:n S**

The same as <:, mutatis mutandis.

*** S <:+ S**

The same as <:, mutatis mutandis.

*** S <:- S**

The same as <:, mutatis mutandis.

A.3 Proof of the factoring lemmas, propositions 7 and 8

This section contains through all of the cases of the factoring lemmas. Many of the cases are immediate, so nothing is written after them. It begins with a few lemmas, before continuing with the factoring results proper.

*** Factoring Lemma 1: S <:- G iff S <: G or S = Dyn**

This is all of the types that are <:- G.

```
if G = B:
   B
   {x:B|t}
   Dyn

if G = Dyn->Dyn
   Dyn -> Dyn
   Dyn

This is all of the types that are <: G.

if G=B:
   B
   {x:B|t}

if G=Dyn->Dyn:
   Dyn->Dyn
```

*** Factoring Lemma 2: S <:- Dyn => S <: Dyn**

By a case analysis.

*** Factoring Lemma 3: Dyn <:+ S => Dyn <: S**

By a case analysis.

*** S <: T implies S <:+ T and S <:- T**

By induction on the structure of the derivation that S <: T.

**** S <: T by rule one. Thus S=T=B.**
**** S <: T by rule two. Thus S=T=Dyn.**
**** S <: T by rule three. Thus S=S'->S'' & T=T'->T''**
By induction.
**** S <: T by rule four. Thus S={x:B|t} and U <: T.**
By induction.
**** S <: T by rule five. Thus T={x:B|t} and x:B<=S |= t**
By induction.
**** S <: T by rule 6. Thus T=Dyn and S <: G**
By induction, we have S <:- G, which gives us S<:-Dyn. S<:+Dyn, since
everything is.

*** S <:+ T and S <:- T imples S <: T**

**** S <:+ T by rule one. Thus S=T=B.**
**** S <:+ T by rule two. Thus T=Dyn.**

***** case 2a. S <:- T by rule 2. Thus S=Dyn.**
***** case 2b. S <:- T by rule 4. Thus S={x:B|t} and B <:- Dyn**

Since S={x:B|t}, we know from by using rules 4 and 6 that S <: T, ie:

```
   B <: B
------------[4]
{x:B|t} <: B
------------[6]
{x:B|t} <: T
```

***** case 2c. S <:- T by rule 6. Thus S <:- G**

By lemma above, either S <: G, and we can use rule 6 of <: and be done, or S=Dyn and Dyn <: Dyn.

**** S <:+ T by rule 3. Thus S=S'->S'' and T=T'->T''.**

***** Case 3a. S <:- T by rule 3.**

By induction.

***** Case 3b. S <:- T by rule 6. Thus S <:- G.**

From the analysis above (and the fact that S = S'->S''), we know that S = Dyn -> Dyn

Since Dyn->Dyn <:+ T'->T'', we know that T' <:- Dyn and Dyn <:+ T''. From lemma 2 and 3, we know that T' <: Dyn and Dyn <: T'', and thus Dyn->Dyn <: T-> T.

**** S <:+ T by rule 4. Thus S={x:B|t} and B <:+ T.**

From rule 6 of <:- we know that B <:- T. Thus by induction we have that B <: T. Now by rule rule 4 of <:, we have S <: T.

**** S <:+ T by rule 5. Thus T={x:B|t} and S <:+ B and x:B<=S |= t.**

***** case 5b. S <:- T by rule 4. Thus S={x:B'|t'} and B' <:- T.**

The only way to derive that B' <:- {x:B|t} is rule 5. Thus B' <:- B. The only way to derive that {x:B'|t'} <:+ B is rule 4 and thus B' <: B. By induction we have that B <: B. Using that, rules 4 and 5 for <: and x:B<=S |= t, we have that S <: T.

***** case 5c. S <:- T by rule 5. Thus S <:- U.**

By induction, we know that S <: U. That plus x:U<=S |= t and rule 5 for <: lets us conclude that S <: T.

***** case 5d. S <:- T by rule 6. Thus S <:- G.**

Since S <:- G, by rule 6 we know that S <:- U. By induction we have that S <: U and then we can apply rule 5 of <: to conclude that

S <: T.

*** S <:n T imples S <:+ T and T <:- S**

**** case 1. S <:n T by rule 1. Thus S = T = B.**
**** case 2. S <:n T by rule 2. Thus T = Dyn.**
**** case 3. S <:n T by rule 3. Thus S = S'->S'' and T = T'->T''**
By induction.
**** case 4. S <:n T by rule 4. Thus S={x:B|t}**
By induction.
**** case 5. S <:n T by rule 5. Thus T={x:B|t} and x:B<=S |= t.**
By induction.

*** S <:+ T and T <:- S imples S <:n T**

**** S <:+ T by rule one. Thus S=T=B.**
**** S <:+ T by rule two. Thus T=Dyn.**
**** S <:+ T by rule 3. Thus S=S'->S'' and T=T'->T''.**

***** 3a. T <:- S by rule 3. Thus T'->T'' <:- S'->S''**
By induction

***** 3b. T <:- S by rule 6. Thus T <:- G.**

From the analysis above and the fact that T = T'->T'', we know that T = Dyn->Dyn and we can derive directly that S'->S'' <:n Dyn->Dyn.

**** S <:+ T by rule 4. Thus S={x:B|t} and B <:+ T.**

***** T <:- S by rule 2. Thus T=Dyn**

Use rule 2 of <:n.

***** T <:- S by rule 4. Thus T={x:B'|t'} and B' <:- S**

There is only one way to conclude that B' <:- {x:B|t}, rule 5. Thus, B' <:- B. There is only one way to conclude that B <:+ {x:B'|t'}, rule 5, which also tells us that we have B <:+ B' and x:B'<=B |= t'. By induction, we know that B <:n B'. By rule 5 of <:n, we have that B <: {x:B'|t'}. By rule 4 of <:n, we have that {x:B|t} <:n {x:B'|t'}.

***** T <:- S by rule 5. Thus T <:- U.**

By induction, we have that T <:n U. By rule 4 of <:n, we can conclude that S <:n T.

***** T <:- S by rule 6. Thus T <:- G**

By rule 6 again we have that T <:- U. By induction we know that U <:n T, and then by rule 4 of <:n we know that S <:n T.

**** S <:+ T by rule 5. Thus T={x:B|t} and S <:+ B and x:B<=S |= t.**

***** T <:- S by rule 4. Thus, B <:- S**

By induction, we have that S <:n B. Thus we have the hypotheses for rule 5 of <:n, and can conclude that S <:n T.

***** T <:- S by rule 5. Thus, S={x:B'|t'}, T <:- B'**

The only way to derive that {x:B|t} <:- B' is by rule 4, and thus we know that B <:- B'. The only way to derive that {x:B'|t'} <:+ B is rule 5 which tells us that B' <:+ B. Thus, by induction, we know that B' <:n B. By rule 4 of <:n we can conclude that S = {x:B'|t'} <:n B, and then by rule 5 of <:n we can conclude that S <:n T.

***** T <:- S by rule 6. Thus T <:- G.**

We know that S <:+ B from the premise of the rule and since B <:- B then B <:- S by rule 6. Thus, by induction we have that S <:n B and by rule 3 of <:n we can conclude that S <:n T.

A.4 Proof of the blame theorem, propositions 9 and 10

Prop 7 from esop submission

Split it up into two propositions, analogous to preservation and progress (thinking of 'safe for' as the thing to be preserved and 'blame(p)' as failure to progress).

*** Preservation: if t is safe for p and t --> t', then t' safe for p.**

Proof proceeds by cases on the reduction rules (note that the second clause of the 'or' above is only used for rule 8).

**** rule 1; no casts change, no |> introduced**
**** rule 2; no casts change, no |> introduced**
**** rule 3; eliminated a cast, no |> introduced**
**** rule 4; preserves the polarity properly, no |> introduced**
**** rule 5; eliminated a cast, no |> introduced**
**** rule 6; turned a cast into an equivalent Dyn_G, no |> introduced**
**** rule 7; no |> introduced**

If the cast is labelled p, we have:
  S -> T <:+ Dyn -> Dyn.
  Dyn -> Dyn <:+ Dyn

If the cast is labelled ~p, we have:
  S -> T is not <:- Dyn, so property trivially holds.

**** rule 8; no |> introduced**

If the cast is labelled p, we have:

Dyn <:+ T imples T = Dyn, or T = {x:Dyn|t} and x:Dyn <= Dyn |= t.
In both cases, we can derive that G <:+ T.

If the cast is labelled ~p, we have: since G <:- G, we know that
G <:- T.

**** rule 9; eliminated a cast, no |> introduced**
**** rule 10;**

If {x:B|t} <:+ S, then B <:+ S. Ditto <:-

There is a |> expression introduced, but the definition of entailment
tells us that it will produce true.

**** rule 11; no casts change, no |> introduced**
**** rule 12; cannot happen, according to the premise**
**** rule 13;**

If {x:B|s} <:+ T, then B <:+ T. Ditto <:-.

***** Progress: if t safe for p, then t -/-> blame(p)**

The only relevant reduction rules are those that end in blame(p),
namely rules 9 and 12.

**** rule 9**

If Dyn <:+ T, then just reading off of the conclusions from all of the
cases of entailment eliminates all but the second and fifth case.

***** Case 2: T = Dyn.**

From the side-condition on this rule, we know that G ~ T does not
hold; but every type is ~ with Dyn. Thus, this reduction rule cannot
fire.

***** Case 5: T = {x:B|t}**

In this case, the premise tells us that Dyn <:+ B, but that is not
derivable. Hence T cannot be {x:B|t}.

**** rule 12.**

The left-hand side of this rule is not safe for p.