Gradual Typing with Unification-Based Inference ; CU-CS-1039-08

Jeremy Siek
University of Colorado Boulder

Manish Vachharajani
University of Colorado Boulder

Follow this and additional works at: https://scholar.colorado.edu/csci_techreports

Recommended Citation
https://scholar.colorado.edu/csci_techreports/970
Gradual Typing with Unification-based Inference

Jeremy G. Siek  
Dept. of Electrical and Computer Engineering  
University of Colorado at Boulder  
425 UCB  
Boulder, CO 80309 USA

Manish Vachharajani  
Dept. of Electrical and Computer Engineering  
University of Colorado at Boulder  
425 UCB  
Boulder, CO 80309 USA

CU Technical Report CU-CS-1039-08  
January 2008
Abstract

Static and dynamic type systems have well-known strengths and weaknesses. *Gradual typing* provides the benefits of both in a single language by giving the programmer control over which portions of the program are statically checked based on the presence or absence of type annotations.

This paper studies the combination of gradual typing and unification-based type inference, with the goal of developing a system that helps programmers increase the amount of static checking in their program. The key question in combining gradual typing and inference is how should the dynamic type of a gradual system interact with the type variables of an inference system. This paper explores the design space and shows why three straightforward approaches fail to meet our design goals. In particular, the combined system should satisfy the criteria for a gradual type system: 1) when a program is unannotated, only a few type errors are detected at compile-time and the rest are detected at run-time, and 2) when the program does not contain dynamic type annotations (implicitly or explicitly), the type system should statically detect all type errors.

This paper presents a new type system based on the idea that a solution for a type variable should be as informative as any type that constrains the variable. We prove that the new type system satisfies the above criteria for a gradual type system. The paper also develops an efficient inference algorithm and proves it sound and complete with respect to the type system.
1 Introduction

Static and dynamic typing have complementary strengths, making them better for different tasks and stages of development. Static typing, used in languages such as Standard ML [18], provides full-coverage type error detection, facilitates efficient execution (since values may remain unboxed and run-time checking of type tags is not needed), and provides machine-checked documentation that is particularly helpful for maintaining consistency when programming in the large. The main drawback of static typing is that the whole program must be well-typed before the program can be run. Typing decisions must be made for all elements of the program, even for ones that have yet to stabilize, and changes in these elements can ripple throughout the program.

In a dynamically typed language, no compile-time checking is performed. Thus, programmers need not worry about types while the overall structure of the program is still in flux. This makes dynamic languages suitable for rapid prototyping. Dynamically typed languages such as Perl, Ruby, Python, and JavaScript are popular for scripting and web applications where rapid development and prototyping is prized above other features. The problem with dynamic languages is that they forgo the benefits of static typing: there is no machine checked documentation, execution is less efficient, and errors are caught only at runtime, often after deployment.

Gradual typing, recently introduced by Siek and Taha [29], enable programmers to mix static and dynamic type checking in a program by providing a convenient way to control which parts of a program are statically checked. The defining properties of a gradual type system are:

1. Programmers may omit type annotations and immediately run the program; run-time type checks are performed to preserve type safety.

2. Programmers may add type annotations to increase static checking. When all variables are annotated, all type errors are caught at compile-time.

A number of researchers have further studied gradual typing over the last two years. Herman, Tomb, and Flanagan [12] developed space-efficient run-time support for gradual typing. Siek and Taha [30] integrated gradual typing with objects and subtyping. Wadler and Findler showed how to perform blame tracking and proved that the well-typed portions of a program can’t be blamed [36]. Herman and Flanagan are adding gradual typing to the next version of JavaScript [11].

An important question, from both a theoretical and practical perspective, has yet to be answered: is gradual typing compatible with type inference? Type inference is common in modern functional languages and is becoming more common in mainstream languages [10, 37]. There are many flavors of type inference: Hindley-Milner inference [17], dataflow-based inference [6], Soft Typing [3], and local inference [24] to name a few. In this paper we study type inference based on unification [28], the foundation of Hindley-Milner inference and the related family of algorithms used in many functional languages [16, 18, 22].

The contributions of this paper are:

1. An exploration of the design space that shows why three straightforward inference approaches do not satisfy the above criteria for a gradual type system (§3). The three approaches are: 1) treat dynamic types as type variables, 2) well-typed after substitution, and 3) ignore dynamic types during unification.

2. A new design based on the idea that the solution for a type variable should be as informative as any type that constrains the variable (§4). We formalize this idea in a type
system (§4.2) and prove that it satisfies the criteria of a gradual type system (§4.3). We
machine checked the proofs in Isabelle/HOL [20]. The formalization and proofs are in
Appendix A.

3. An inference algorithm for the above type system (§5). We prove that the algorithm
is sound and complete with respect to the type system and that the algorithm has al-
most linear time complexity (§5.3). The algorithm does not infer types that introduce
unnecessary cast errors.

Before the main technical developments, we review gradual typing as well as traditional
unification-based inference (§2). After the main body of the paper, we place our work in
relation to the relevant literature (§6) and conclude (§7).

2 Review of Gradual Typing and Inference

We review gradual typing in the absence of type inference, showing examples in a hypothetical
variant of Objective Caml [16] that supports gradual typing but not type inference. We then
review type inference in the absence of gradual typing.

A Review of Gradual Typing  The incr function listed below has a parameter x and returns
x + 1. The parameter x does not have a type annotation so the gradual type system delays
checks concerning x inside the incr function until run-time, just as a dynamically typed language
would.

\begin{verbatim}
let incr x = x + 1
let a:int = 1
incr a
\end{verbatim}

More precisely, because the parameter x is not annotated the gradual type system gives it the
dynamic type, written ? for short.

Now suppose the + operator expects arguments of type int. The gradual type system allows
an implicit coercion from type ? to int. This kind of coercion could fail (like a down cast) and
therefore must be dynamically checked. In some statically-typed languages, such as ML, implicit
coeercions are forbidden; in many object-oriented languages, such as Java, implicit up-casts are
allowed (they never fail) but not implicit down-casts. Allowing implicit coercions that may fail
is the distinguishing feature of gradual typing and gives it the flavor of dynamic typing.

To facilitate the migration of code from dynamic to static checking, gradual typing allows
for a mixture of the two and provides seamless interaction between them. In the example above,
we define a variable a of type int, and invoke the dynamically typed incr function. Here the
gradual type system allows an implicit coercion from int to ?. This is a safe coercion—it can
never fail at run-time—however the run-time system needs to remember the type of the value
so that it can check the type when it casts back to int inside of incr.

Gradual typing also allows implicit coercions among more complicated types, such as function
types. In the following example, the map function has a parameter f annotated with the
function type (int \rightarrow int) and a parameter l with type int list.

\begin{verbatim}
let rec map (f:int\rightarrow int) (l:int list) = ...
let incr x = x + 1
let a:int = 1
map incr [1; 2; 3] (* OK *)
map a [1; 2; 3] (* compile time type error *)
\end{verbatim}
The function call `map incr [1; 2; 3]` is allowed by the gradual type system, even though the type of the argument `incr ? → int` differs from the type of the parameter `(int → int)`. The type system compares the two types structurally and allows the two types to differ in places where one of the types has a `?`. Thus, the function call is allowed because the return types are equal and there is a `?` in one of the parameter types. In contrast, `map a [1; 2; 3]` elicits a compile-time error because argument `a` has type `int` whereas `f` is annotated with a function type.

When a program is fully annotated, that is, when all the program variables are annotated with types that include no `?` types, the gradual type system catches at compile-time all the errors that a fully-static type system would.

More formally, the main idea of gradual typing is to replace the use of type equality with a relation called type consistency, written `∼` for short. The intuition behind type consistency is to check whether the two types are equal in the parts where both types are known. The following are a few examples.

```
int ∼ int  int ⊬ bool  ? ∼ int  int ∼ ?
int → ? ∼? → int  int → ? ∼ int → bool
int → ? ⊬ bool → ?  int → int ⊬ int → bool
```

The following is an inductive definition of the consistency relation. This relation is reflexive, symmetric, but not transitive.

**Type Consistency**

\[
\begin{align*}
(CRefl) & \quad \frac{}{\tau \sim \tau} \\
(CFun) & \quad \frac{\tau_1 \sim \tau_2 \quad \rho_1 \sim \rho_2}{\tau_1 \rightarrow \rho_1 \sim \tau_2 \rightarrow \rho_2} \\
(CDR) & \quad \frac{}{\tau \sim ?} \\
(CDL) & \quad \frac{}{? \sim \tau}
\end{align*}
\]

The syntax of the gradually typed lambda calculus (\(\lambda^?\)) is shown below and the type system is reproduced in Figure 1. A gradual type system uses type consistency where a simple type system uses type equality. For example, the (App2) rule in the gradually typed lambda calculus [29] requires that the argument type \(\tau_2\) be consistent with the parameter type \(\tau_1\).

**Syntax for \(\lambda^?\)**

```
Variables \(x, y \in X\)
Ground Types \(\gamma \in G \supseteq \{bool, int, unit\}\)
Constants \(c \in C \supseteq \{true, false, succ, 0, (), fix[\tau]\}\)
Types \(\tau \quad ::= \quad ? \mid \gamma \mid \tau \rightarrow \tau\)
Expressions \(e \quad ::= \quad x \mid c \mid e \mid e \mid \lambda x. \tau. \ e\)
\lambda x. e \quad \equiv \quad \lambda x?:e
```

This type system meets both criteria for a gradual type system discussed in §1: the first because the consistency relation allows implicit coercions both to and from the dynamic type, the second because when there are no `?`s in the program (either explicitly or implicitly), this type system is equivalent to a fully static type system. The consistency relation collapses to equality when there are no `?`s: for any \(\sigma\) and \(\tau\) that contain no `?`s, \(\sigma \sim \tau\) iff \(\sigma = \tau\).

**Review of Unification-based Type Inference** Type inference allows programmers to omit type annotations but still enjoy the benefits of static type checking. For example, the following
is a well-typed Objective Caml program. The inference algorithm deduces that the type of function \( f \) is \( \text{int} \rightarrow \text{int} \).

\[
\text{# let } f \ x = x + 1 ; ;
\text{val } f : \text{int} \rightarrow \text{int} = (\text{fun})\ (* \text{Output of inference} \*)
\]

The type inference problem is formulated by attaching a type variable, an \textit{unknown}, to each location in the program. The job of the inference algorithm is to deduce a solution for these variables that obeys the rules of the type system. So, for example, the following is the above program annotated with type variables.

\[
\text{let } f \alpha x \beta = (x \gamma + \delta_1 \chi) \rho
\]

The inference algorithm models the rules of a type system as equations that must hold between the type variables. For example, the type \( \beta \) of the parameter \( x \) must be equal to the type \( \gamma \) of the occurrence of \( x \) in the body of \( f \). The parameter types of \( + \) (both are \( \text{int} \)) must be equal to the argument types \( \gamma \) and \( \chi \), and the return type of \( + \), also \( \text{int} \), must be equal to \( \rho \). Ultimately, the type \( \alpha \) of \( f \) must be equal to the function type \( \beta \rightarrow \rho \) formed from the parameter type \( \beta \) and the return type \( \rho \). This set of equations can be solved by standard unification \[28\].

A substitution maps type variables to types and can be naturally extended to map types to types. The unification algorithm computes a substitution \( S \) such that for each equation \( \tau_1 = \tau_2 \), we have \( S(\tau_1) = S(\tau_2) \).

A natural setting in which to formalize type inference is the simply typed lambda calculus with type variables (\( \lambda^\alpha \)). The syntax is similar to \( \lambda^? \), but with type variables and no dynamic type. The standard type system for the simply typed lambda calculus \[23\] is reproduced in Figure 2. The extension of this type system to handle type variables, given below, is also standard \[23\].

**Definition 1.** A term \( e \) of \( \lambda^\alpha \) is \textbf{well-typed} in environment \( \Gamma \) if there is a substitution \( S \) and a type \( \tau \) such that \( S(\Gamma) \vdash S(e) : \tau \).

We refer to this approach to defining well-typedness for programs with type variables as \textit{well-typed after substitution}.

An inference algorithm for \( \lambda^\alpha \) can be expressed as a two-step process \[8, 23, 38\] that generates a set of constraints (type equalities) from the program and then solves the set of equalities with unification. Constraint generation for \( \lambda^\alpha \) is defined in Figure 3. The soundness and completeness of the inference algorithm with respect to the type system has been proved in the literature \[23, 38\].
\[
\begin{align*}
\Gamma(x) &= \tau_1 \\
\Gamma \vdash x : \tau_1 \\
\Gamma \vdash c : \text{typeof}(c) \\
\Gamma \vdash e_1 : \tau_1 \rightarrow \tau_2 \\
\Gamma \vdash e_2 : \tau_1 \\
\Gamma(x \mapsto \tau_1) \vdash e : \tau_2 \\
\Gamma \vdash \lambda x : \tau_1. e : \tau_1 \rightarrow \tau_2
\end{align*}
\]

Figure 2: The type system of the simply typed \(\lambda\)-calculus.

\[
\begin{align*}
\Gamma(x) &= \tau \\
\Gamma \vdash x : \tau \mid \{\} \\
\Gamma \vdash c : \text{typeof}(c) \mid \{\} \\
\Gamma \vdash e_1 : \tau_1 \mid C_1 \\
\Gamma \vdash e_2 : \tau_2 \mid C_2 \quad (\beta \text{ fresh}) \\
\Gamma \vdash e_1 e_2 : \beta \mid (\tau_1 = \tau_2 \rightarrow \beta) \cup C_1 \cup C_2 \\
\Gamma(x \mapsto \tau) \vdash e : \rho \mid C \\
\Gamma \vdash \lambda x : \tau. e : \tau \rightarrow \rho \mid C
\end{align*}
\]

Figure 3: The definition of constraint generation for \(\lambda^\alpha\).

In §4 we combine inference with gradual typing and need to treat type variables with special care, but if we follow the well-typed-after-substitution approach, type variables are substituted away before the type system is consulted. As an intermediate step towards integration with gradual typing, we give an equivalent definition of well-typed terms for \(\lambda^\alpha\) that combines the substitution \(S\) with the type system. The type system is shown in Figure 4 and the judgment has the form \(S; \Gamma \vdash e : \tau\) which reads: \(e\) is well-typed because \(S\) and \(\tau\) are a solution for \(e\) in \(\Gamma\).

Formally, we use the following representation for substitutions, which is common in mechanized formalizations [19].

**Definition 2.** A substitution is a total function from type variables to types and its \(\text{dom}\) consists of the variables that are not mapped to themselves. Substitutions extend naturally to types, typing environments, and expressions. The \(\circ\) operator composes two substitutions.

Theorem 1 states that the two type systems are equivalent, and relies on the following two lemmas. The function \(\text{FTV}\) returns the free type variables within a type, type environment, or expression.

**Lemma 1.** If \(S(\Gamma) \vdash S(e) : \tau\) and \(S\) is idempotent then \(S(\tau) = \tau\).

**Proof.** Observe that if \(S(\Gamma) \vdash S(e) : \tau\) then \(\text{FTV}(\tau) \cap \text{dom}(S) = \emptyset\). Furthermore, if \(S\) is idempotent then \(\text{FTV}(\tau) \cap \text{dom}(S) = \emptyset\) implies \(S(\tau) = \tau\).

**Lemma 2.** If \(S\) idempotent and \(S(\tau) = \tau_1 \rightarrow \tau_2\) then \(S(\tau_2) = \tau_2\).

**Proof.** We have \(\tau_1 \rightarrow \tau_2 = S(\tau) = S(S(\tau)) = S(\tau_1 \rightarrow \tau_2) = S(\tau_1) \rightarrow S(\tau_2)\). Thus \(\tau_2 = S(\tau_2)\).
Theorem 1. The two type systems for $\lambda^\alpha$, are equivalent.

1. Suppose $S$ is idempotent. If $S(\Gamma) \vdash S(e) : \tau$, then there is a $\tau'$ such that $S; \Gamma \vdash e : \tau'$ and $S(\tau') = \tau$.

2. If $S; \Gamma \vdash e : \tau$, then $S(\Gamma) \vdash S(e) : S(\tau)$.

Proof. 1. $S(\Gamma) \vdash S(e) : \tau \implies S(\Gamma) \vdash S(e) : S(\tau)$ by Lemma 1. We prove by induction that $S(\Gamma) \vdash S(e) : S(\tau)$ implies there is a $\tau'$ such that $S; \Gamma \vdash e : \tau'$ and $S(\tau') = S(\tau)$. We use Lemma 1 in the (App) case and Lemma 2 in the (Abs) case. Then using Lemma 1 once more gives us $S(\tau') = \tau$.

2. The proof is a straightforward induction on $S; \Gamma \vdash e : \tau$. \hfill $\square$

3 Exploration of the Design Space

We investigate three straightforward approaches to integrate gradual typing and type inference. In each case we give examples of programs that should be well-typed but are rejected by the approach, or that should be ill-typed but are accepted by the approach.

Dynamic Types as Type Variables  A simple approach is to replace every occurrence of ? in the program with a fresh type variable and then do constraint generation and unification as presented in §2. The resulting system is fully static, not gradual. Consider the following program.

```plaintext
let z = ...
let f (x : int) = ...
let g (y : bool) = ...
let h (a : ?) = if z then f a else g a
```

Variable $a$ has type ? and so a fresh type variable $\alpha$ would be introduced for its type. The inference algorithm would deduce from the function applications $f a$ and $g a$ that $\alpha = \text{int}$ and $\alpha = \text{bool}$ respectively. There is no solution to these equations, so the program would be rejected with a static type error. However, the program would run without error in a dynamically typed language given an appropriate value of $z$ and input for $h$. Furthermore, this program type checks in the gradual type system of Figure 1 so it ought to remain valid in the presence of type inference.
The next example exhibits a different problem: the inference algorithm may not find concrete solutions for some variables and therefore indicate polymorphism in cases where there shouldn’t be.

```
let f (x : int) (g : ? → ?) =
g x
```
Generating fresh type variables for the ?s gives us \( g : \alpha \rightarrow \beta \). Let \( \gamma \) be the type variable for the return type of \( f \) and the type of the expression \( g \times \). The only equation constraining \( \gamma \) is \( \gamma = \beta \), so the return type of \( f \) is inferred to be \( \beta \). But if \( f \) is really polymorphic in \( \beta \) it should behave uniformly for any choice \( \beta \) [27, 35]. Suppose \( g \) is the identity function. Then \( f \) raises a cast error if \( \beta = \text{bool} \) but not if \( \beta = \text{int} \).

**Ignore Dynamic Types During Unification** Yet another straightforward approach is to adapt unification by simply ignoring any unification of the dynamic type with any other type. However, this results in programs with even more unsolved variables than in the approach described above. Consider again the following program.

```
let f (x : int) (g : ? → ?) =
    g x
```
From the function application, the inference algorithm would deduce \( ? \rightarrow ? = \text{int} \rightarrow \beta \), where \( \beta \) is a fresh variable representing the result type of the application \( g \times \). This equality would decompose to \( ? = \text{int} \) and \( ? = \beta \). However, if the unification algorithm does not do anything with \( ? = \beta \), we end up with \( \beta \) as an unsolved variable, giving the impression that \( f \) is parametric in \( \beta \), which is certainly not the case. Some choices for \( \beta \) can cause runtime cast errors whereas other choices do not.

**Well-typed After Substitution** In §2 we presented the standard type system for \( \lambda^\omega \), saying that a program is well typed if there is some substitution that makes the program well typed in \( \lambda_\omega \). We could do something similar for gradual typing, saying that a gradually typed program with variables is well typed if there exists a substitution that makes it well typed in \( \lambda^\omega \). (Figure 1).

It turns out that this approach is too lenient. Recall that to satisfy criteria 2 of gradual typing, for fully annotated programs the gradual type system should act like a static type system. Consider the following program that would not type check in a static type system because \( \alpha \) cannot be both an int and a function.

```
let f (g: α) = g 1
f 1
```
Applying the substitution \( \{ \alpha \mapsto ? \} \) produces a program that is well-typed in \( \lambda^\omega \).

The next example shows a less severe problem, although it still undermines the purpose of type inference, which is to help programmers increase the amount of static typing in their programs.

```
let x:α = x + 1
```
Again, the substitution \( \{ \alpha \mapsto ? \} \) is allowed, but it does not help the programmer. Instead, one wants to find out that \( \alpha = \text{int} \). In general, we need to be more careful about where \( ? \) is allowed as the solution for a type variable.

However, we cannot altogether disallow the use of \( ? \) in solutions because we want to avoid introducing runtime cast errors. Consider the program
let f (x:?) =  
  let y:α = x in y

Here, the only appropriate solution for α is the dynamic type. Any other choice introduces an implicit cast to that type, which causes a runtime cast error if the function is applied to a value whose type does not match our choice for α. Suppose we choose α = int. This type checks in \( \lambda^\top \) because int is consistent with ?, but if the function is called with a boolean argument, a runtime cast error occurs.

The problem with the well-typed-after-substitution approach is that it can “cheat” by assigning ? to a type variable and thereby allow programs to type check that should not. Thus, we need to prevent the type system from adding in arbitrary ?s. On the other hand, we need to allow the propagation of ?s that are already in program annotations.

4 A Type System for \( \lambda^\top \)

Loosely, we say that types with more question marks are less informative. The main idea of our new type system is to require the solution for a type variable to be as informative as any type that constrains the type variable. This prevents a solution for a variable from introducing dynamic types that do not already appear in program annotations. Formally, information over types is characterized by the less or equally informative relation, written \( \sqsubseteq \). This relation is just the partial order underlying the \( \sim \) relation\(^1\). An inductive definition of \( \sqsubseteq \) is given below.

Less or Equally Informative

\[
\begin{align*}
(LID) \quad & ? \sqsubseteq \tau \\
(LIRefl) \quad & \tau \sqsubseteq \tau \\
(LIFun) \quad & \tau_1 \sqsubseteq \tau_3 \\
& \tau_2 \sqsubseteq \tau_4 \\
& \tau_1 \to \tau_2 \sqsubseteq \tau_3 \to \tau_4 
\end{align*}
\]

The \( \sqsubseteq \) relation is a partial order that forms a semi-lattice with ? as the bottom element and \( \sqsubseteq \) extends naturally to substitutions.

We revisit some examples from §3 and show how using the \( \sqsubseteq \) relation gives us the ability to separate the good programs and good solutions from the bad. Recall the following example that should be rejected but was not using the well-typed-after-substitution approach.

let f (g:α) = g 1
f 1

In our approach, the application of g to 1 introduces the constraint \( \text{int} \to \beta_0 \sqsubseteq \alpha \) (where \( \beta_0 \) is a fresh variable generated for the result of the application) because g is being used as a function from \( \text{int} \) to \( \beta_0 \). Likewise, the application of f to 1 introduces the constraint \( \text{int} \to \beta_1 \sqsubseteq \alpha \to \beta_0 \) which implies \( \text{int} \sqsubseteq \alpha \). There is no solution to these constraints on \( \alpha \) so the program is rejected.

In the next example, the only solution for \( \alpha \) should be \( \text{int} \).

let x:α = x + 1

Indeed, in our approach we have the constraint \( \text{int} \sqsubseteq \alpha \) whose only solution is \( \alpha = \text{int} \).

In the third example, the type system should allow \( \alpha = ? \) as a solution.

\(^1\) Each relation is definable in terms of the other: we have \( \tau_1 \sim \tau_2 \) iff there is a \( \tau_3 \) such that \( \tau_1 \sqsubseteq \tau_3 \) and \( \tau_2 \sqsubseteq \tau_3 \), and in the other direction, \( \tau_1 \sqsubseteq \tau_2 \) iff for any \( \tau_3 \), \( \tau_2 \sim \tau_3 \) implies \( \tau_1 \sim \tau_3 \).
let f (x:? =
let y:α = x in y

Indeed, we have the constraint ? ⊑ α, which allows α = ? as a solution. In this case the type system allows many solutions, some of which, as discussed in §3 may introduce unnecessary casts. In our design, the inference algorithm is responsible for choosing a solution that does not introduce unnecessary casts. It will do this by choosing the least informative solution allowed by the type system. This means the inference algorithm chooses the least upper bound of all the types that constraint a type variable as the solution for that variable.

The following program further illustrates how the ⊑ relation constrains the set of valid solutions.

let f (g:?→int) (h:int→?) = ...
let k (y:α) = f y y

The parameter y is annotated with type variable α and is used in two places, one that expects ? → int and the other that expects int → ?. So we have the constraints ? → int ⊑ α and int → ? ⊑ α, whose only solution is α = int → int.

Constraints on type variables can also arise from constraints on compound types that contain type variables. For example, in the following program, we need to delve under the function type to uncover the constraint that int ⊑ α.

let g (f:int→int) = f 1
let h (f:α→α) = g f

In the next subsection we define how this works in our type system.

4.1 The Consistent-equal and Consistent-less Judgments

To formalize the notions of constraints between arbitrary types, we introduce two judgments: consistent-equal, which has the form $S \models \tau \simeq \tau$ and consistent-less, which has the form $S \models \tau \sqsubseteq \tau$. The two judgments are defined in Figure 5. The consistent-equal judgment is similar to the type consistency relation ~ except that \( \simeq \) gives special treatment to variables. When a variable occurs on either side of the \( \simeq \), the substitution for that variable is required to produce a type that is as informative as the other type according to the consistent-less judgment. The consistent-less judgment is similar to the \( \sqsubseteq \) relation except that it also gives special treatment to variables. When a variable appears on the left, the substitution for that variable is required to be equal to the type on the right. (There is some asymmetry in the $S \models \tau \sqsubseteq \tau$ judgment. The substitution is applied to type of the left and not the right because the substitution has already been applied to the type on the right.)

We illustrate the rules for consistent-equal and consistent-less with the following example.

$S \models \text{int} \rightarrow \alpha \simeq ? \rightarrow (\beta \rightarrow (\text{int} \rightarrow ?))$

What choices for S satisfies the above constraint? Applying the inverse of the (CEF\textsc{un}) rule we have

$S \models \text{int} \simeq ?, \ S \models \alpha \simeq \beta \rightarrow (\text{int} \rightarrow ?)$

The first constraint is satisfied by any substitution using rule (CED\textsc{r}), but the second constraint is satisfied when

$S \models \beta \rightarrow (\text{int} \rightarrow ?) \sqsubseteq S(\alpha)$
Figure 5: The consistent-equal and consistent-less judgments.

using rule (CEVL). There are many choices for \( \alpha \), but whichever choice is made restricts the choices for \( \beta \). Suppose

\[
\{ \alpha \mapsto (\? \to \text{bool}) \to (\text{int} \to \text{bool}) \} \subseteq S
\]

Then we have

\[
S \models \beta \to (\text{int} \to \?) \subseteq (\? \to \text{bool}) \to (\text{int} \to \text{bool})
\]

and applying the inverse of (CLFun) yields

\[
S \models \beta \subseteq \? \to \text{bool}, \quad S \models \text{int} \to \? \subseteq \text{int} \to \text{bool}
\]

The second constraint is satisfied by any substitution using (CLFun), (CLG), and (CLDL), but the first constraint is only satisfied when

\[
S(\beta) = (\? \to \text{bool})
\]

according to rule (CLVAR).

A key property of the \( \models \cdot \simeq \cdot \) judgment is that it allows the two types to differ with respect to \?, but if both sides are variables, then their solutions must be equal, i.e., if \( S \models \alpha \simeq \beta \) then \( S(\alpha) = S(\beta) \). This is why \( \{ \alpha \mapsto \text{int} \} \) is a solution for the following program but \( \{ \alpha \mapsto ? \} \) is not.

\[
\begin{align*}
\text{let } f(x: \alpha) = \\
\text{let } y: \beta = x \text{ in } y + 1
\end{align*}
\]

**Proposition 1.** (Properties of \( S \models \tau \simeq \tau \) and \( S \models \tau \subseteq \tau \))

1. \( S \models \tau_1 \subseteq \tau_2 \) and \( S \models \tau_3 \subseteq \tau_2 \) implies \( S \models \tau_1 \simeq \tau_3 \).

2. Suppose \( \tau_1 \) and \( \tau_3 \) do not contain \?s. Then \( S \models \tau_1 \subseteq \tau_2 \) and \( S \models \tau_1 \simeq \tau_3 \) implies \( S \models \tau_3 \subseteq \tau_2 \).
3. If \( \tau_1 \) and \( \tau_2 \) contain no ?s and \( S \vdash \tau_1 \simeq \tau_2, S(\tau_1) = S(\tau_2) \).

4. If \( \tau_1 \) contains no ?s and \( S \vdash \tau_1 \sqsubseteq \tau_2, S(\tau_1) = \tau_2 \).

5. If \( S \vdash \tau_1 \simeq \tau_2 \rightarrow \beta \), then either \( \tau_1 = ? \) or there exist \( \tau_{11} \) and \( \tau_{12} \) such that \( \tau_1 = \tau_{11} \rightarrow \tau_{12} \), \( \tau_{11} \sim S(\tau_2) \), and \( \tau_{12} \sqsubseteq S(\beta) \).

6. If \( \text{FTV}(\tau_1) = \emptyset \) and \( \text{FTV}(\tau_2) = \emptyset \), \( S \vdash \tau_1 \simeq \tau_2 \) iff \( \tau_1 \sim \tau_2 \).

7. If \( \text{FTV}(\tau_1) = \emptyset \), then \( S \vdash \tau_1 \sqsubseteq \tau_2 \) iff \( \tau_1 \sqsubseteq \tau_2 \).

### 4.2 The Definition of the Type System

We formalize our new type system in the setting of the gradually typed lambda calculus with the addition of type variables (\( \lambda^\omega \)). As in \( \lambda^\omega \), a parameter that is not annotated is implicitly annotated with the dynamic type. This favors programs that are mostly dynamic. When a program is mostly static, it would be beneficial to instead interpret variables without annotations as being annotated with unique type variables. This option can easily be offered as a command-line compiler flag.

With the consistent-equal judgment in hand we are ready to define the type system for \( \lambda^\omega \) with the judgment \( S; \Gamma \vdash e : \tau \), shown in Figure 6. The crux of the type system is the application rule (\( S\text{App} \)). We considered a couple of alternatives before arriving at this rule. First we tried to borrow the (SApp) rule of \( \lambda^\omega \) (Figure 4) but replace \( S(\tau_1) = S(\tau_2 \rightarrow \tau_3) \) with \( S \vdash \tau_1 \simeq \tau_2 \rightarrow \tau_3 \):

\[
S; \Gamma \vdash f e_1 : \tau_1 \quad S; \Gamma \vdash g e_2 : \tau_2 \quad S \vdash \tau_1 \simeq \tau_2 \rightarrow \tau_3
\]

This rule is too lenient: \( \tau_3 \) may be instantiated with ? which allows too many programs to type check. Consider the following program.

\[
\lambda f : \text{int} \to \text{int}. \lambda g : \text{int} \to \text{bool}. f \ (g \ 1)
\]

The following is a derivation for this program. The problem is that the application \( (g \ 1) \) can be given the type ? because \( \{ \} \vdash \text{int} \to \text{bool} \simeq \text{int} \to ? \). Let \( \Gamma_0 \) and \( \Gamma_1 \) be the environments defined as follows.

\[
\Gamma_0 = \{ f : \text{int} \to \text{int} \}
\]

\[
\Gamma_1 = \Gamma_0(g \mapsto (\text{int} \to \text{bool}))
\]

Then we have

\[
\{ \}; \Gamma_1 \vdash g : \text{int} \to \text{bool}
\]

\[
\{ \}; \Gamma_1 \vdash g \ 1 : \text{int}
\]

\[
\{ \}; \Gamma_1 \vdash f : \text{int} \to \text{int}
\]

\[
\{ \}; \Gamma_1 \vdash g \ 1 : ?
\]

\[
\{ \}; \Gamma_1 \vdash (f \ (g \ 1)) : \text{int}
\]

\[
\{ \}; \Gamma_0 \vdash (\lambda g : \text{int} \to \text{bool}. f \ (g \ 1)) : \text{int}
\]

\[
\{ \}; \Gamma_0 \vdash (\lambda f : \text{int} \to \text{int}. \lambda g : \text{int} \to \text{bool}. f \ (g \ 1)) : \text{int}
\]

The second alternative we explored was to borrow the (App1) and (App2) rules from \( \lambda^\omega \), replacing \( \tau_1 \sim \tau_2 \) with \( S \vdash \tau_1 \simeq \tau_2 \).

\[
S; \Gamma \vdash e_1 : ?
\]

\[
S; \Gamma \vdash e_2 : \tau
\]

\[
S; \Gamma \vdash e_1 : ?
\]

\[
S; \Gamma \vdash e_2 : ?
\]

\[
S; \Gamma \vdash e_1 : \tau_1 \rightarrow \tau_3
\]

\[
S; \Gamma \vdash e_2 : \tau_2
\]

\[
S \vdash \tau_1 \simeq \tau_2
\]

\[
S; \Gamma \vdash e_1 : \tau_3
\]

\[
S; \Gamma \vdash e_2 : \tau_3
\]
This alternative also accepts too many programs. Consider the following erroneous program: 
\((\lambda x: \alpha. (x 1)) 1)\). With the substitution \(\{\alpha \mapsto ?\}\) this program is well-typed using the first application rule for both applications.

The problem with both of the above approaches is that they allow the type of an application to be \(?\), thereby adding an extra \(?\) that was not originally in the program. We can overcome this problem by leveraging the definition of the \(\simeq\) judgment, particularly with respect to how it treats type variables: it does not allow the solution for a variable to contain more \(?\)s than the types that constrain it. With this intuition we define the \((\text{GApp})\) rule as follows.

\[
\frac{S; \Gamma \vdash e_1 : \tau_1 \quad S; \Gamma \vdash e_2 : \tau_2}{S; \Gamma \vdash e_1 e_2 : \beta} \quad (\beta \text{ fresh})
\]

The type of the application is expressed using a type variable instead of a metavariable. This subtle change places a more strict requirement on the variable.

Let us revisit the previous examples and show how this rule correctly rejects them. For the first example

\[
\lambda f: \text{int} \to \text{int}. \lambda g: \text{int} \to \text{bool}. f (g 1)
\]

we have the constraint set

\[
\{\text{int} \to \text{bool} \simeq \text{int} \to \beta_1, \text{int} \to \text{int} \simeq \beta_1 \to \beta_2\}
\]

which does not have a solution because \(\beta_1\) must be the upper bound of \(\text{int}\) and \(\text{bool}\) but there is no such upper bound. The second example, \((\lambda x: \alpha. (x 1)) 1)\), gives rise to the following set of constraints

\[
\{\alpha \simeq \text{int} \to \beta_1, \alpha \to \beta_1 \simeq \text{int} \to \beta_2\}
\]

which does not have a solution because \(\alpha\) would have to be the upper bound of \(\text{int} \to \beta_1\) and \(\text{int}\).

### 4.3 Properties of the Type System for \(\lambda_\alpha\)

When there are no type variable annotations in the program, the type system for \(\lambda_\alpha\) is sound with respect to \(\lambda_\alpha\).

**Theorem 2.** Suppose \(\text{FTV}(\Gamma) = \emptyset\) and \(\text{FTV}(e) = \emptyset\). If \(S; \Gamma \vdash e : \tau\), then \(\exists \tau'. S; \Gamma \vdash e : \tau'\) and \(\tau' \subseteq S(\tau)\).
Proof. The proof is by induction on the typing derivations.

The type system for $\lambda_\to^?\alpha$ is stronger (accepts strictly fewer programs) than the alternative type system that says there must be a substitution $S$ that makes the program well-typed in $\lambda_\to^\alpha$ (Figure 1).

**Theorem 3.**

1. If $S; \Gamma \vdash g e : \tau$ then there is a $\tau'$ such that $S(\Gamma) \vdash_g S(e) : \tau'$ and $\tau' \sqsubseteq S(\tau)$.
2. If $S(\Gamma) \vdash_g S(e) : \tau$ then it is not always the case that there is a $\tau'$ such that $S; \Gamma \vdash_g e : \tau'$.

**Proof.** 1. The proof is by induction on the derivation of $S; \Gamma \vdash_g e : \tau$. The case for (GApp) uses Proposition 1, items 2 and 5.

2. Here is a counter example: $(\lambda x : \alpha. x 1) 1$.

When there are no $?$s in the program, a well-typed $\lambda_\to^?\alpha$ program is also well-typed in the completely static type system of $\lambda_\to^\alpha$. The contrapositive of this statement says that $\lambda_\to^?\alpha$ catches all the type errors that are caught by $\lambda_\to^\alpha$.

**Theorem 4.** If $e \in \lambda_\to^\alpha$ and $(\forall \alpha. \Gamma(\alpha) = \tau \implies \tau \in \lambda_\to^\alpha)$ then $S; \Gamma \vdash_g e : \tau$ implies $S; \Gamma \vdash e : \tau$ and $\tau \in \lambda_\to^\alpha$.

**Proof.** The proof is by induction on the derivation of $S; \Gamma \vdash_g e : \tau$. The case for (GApp) uses Proposition 1 item 3.

5 **A Type Inference Algorithm for $\lambda_\to^?\alpha$**

The inference algorithm we develop for $\lambda_\to^?\alpha$ follows a similar outline to that of the algorithm for $\lambda_\to^\alpha$ we presented in Section 2. We generate a set of constraints from the program and then solve the set of constraints. The main difference is that we generate $\simeq$ constraints instead of type equalities, which requires changes to the constraint solver (the unification algorithm).

The classic unification algorithm is not suitable for solving $\simeq$ constraints. Suppose we have the constraint \{ $\alpha \to \alpha \simeq ? \to \text{int}$ \}. The unification algorithm would first unify $\alpha$ and $?$ and substitute $?$ for $\alpha$ on the other side of the $\to$. But $?$ is not a valid solution for $\alpha$ according to the consistent-equal relation: it is not the case that $\text{int} \sqsubseteq ?$. The problem with the classic unification algorithm is that it treats the first thing that unifies with a variable as the final solution and eagerly applies substitution. To satisfy the $\simeq$ relation, the solution for a variable must be an upper bound of all the types that unify with the variable.

The main idea of our new algorithm is that for each type variable $\alpha$ we maintain a type $\tau$ that is a lower bound on the solution of $\alpha$ (i.e. $\tau \sqsubseteq \alpha$). (In contrast, inference algorithms for subtyping maintain both lower and upper bounds [26].) When we encounter another constraint $\alpha \simeq \tau'$, we move the lower bound up to be the least upper bound of $\tau$ and $\tau'$. This idea can be integrated with some care into a unification algorithm that does not rely on substitution. The algorithm we present is a variant of Huet’s almost linear algorithm [13, 15]. We could have adapted Paterson and Wegman’s linear algorithm [21] at the expense of a more detailed and less clear presentation.
5.1 Constraint Generation

The constraint generation judgment has the form $\Gamma \vdash_g e : \tau \mid C$, where $C$ is the set of constraints. The constraint generation rules are given in Figure 7 and are straightforward to derive from the type system (Figure 6). The main change is that the side condition on the (GApp) rule becomes a generated constraint on the (CApp) rule. The meaning of a set of these constraints is given by the following definition.

**Definition 3.** A set of constraints $C$ is **satisfied** by a substitution $S$, written $S \models C$, iff for any $\tau_1 \simeq \tau_2 \in C$ we have $S \models \tau_1 \simeq \tau_2$.

We use one of the previous examples to illustrate constraint generation and, in the next subsection, constraint solving.

$\lambda f : (? \rightarrow \text{int}) \rightarrow (\text{int} \rightarrow ?) \rightarrow \text{int}. \lambda y : \alpha. f y y$

We generate the following constraints from this program.

$\{ (? \rightarrow \text{int}) \rightarrow (\text{int} \rightarrow ?) \rightarrow \text{int} \simeq \alpha \rightarrow \beta_1, \beta_1 \simeq \alpha \rightarrow \beta_2 \}$

Because of the close connection between the type system and constraint generation, it is straightforward to show that the two are equivalent.

**Lemma 3.** Given that $\Gamma \vdash e : \tau \mid C$, $S \models C$ is equivalent to $S; \Gamma \vdash_g e : \tau$.

**Proof.** Both directions are proved by induction on the derivation of the constraint generation.

5.2 Constraint Solver

Huet’s algorithm uses a graph representation for types. For example, the type $\alpha \rightarrow (\alpha \rightarrow \text{int})$ is represented as the node $u$ in the following graph.

```
  u
 / \  /
vα  xint
  \ /  \
  w
```

Figure 7: The definition of constraint generation for $\lambda^\alpha_{\alpha}$. 
Huet used a graph data structure that conveniently combines node labels and out-edges, called the “small term” approach [13, 25]. Each node is labeled with a type, but the type is small in that it consists of either a ground type such as int or a function type (→) whose parameter and return type are nodes instead of types. For example, the above graph is represented by the following stype function from nodes to shallow types.

\[
\begin{align*}
stype(u) &= v \rightarrow w & stype(v) &= \text{var} \\
stype(w) &= v \rightarrow x & stype(x) &= \text{int}
\end{align*}
\]

We sometimes write the stype of a node as a subscript, such as \( u_{\text{int}} \), and \( x_{\text{int}} \). Also, when the identity of a node is not important we sometimes just write the stype label in place of the node (e.g., int instead of \( x_{\text{int}} \)).

Huet’s algorithm uses a union-find data structure [31] to maintain equivalence classes among nodes. The operation \( \text{find}(u) \) maps node \( u \) to its representative node and performs path compression to speed up later calls to \( \text{find} \). The operation \( \text{union}(u,v,f) \) merges the classes of \( u \) and \( v \). If the argument to \( f \) is true then \( u \) becomes the representative of the merged class. Otherwise, the representative is chosen based on which class contains more elements, to reduce time complexity.

The definition of our solve algorithm is in Figure 8. We defer discussion of the copy_dyn used on the first line. In each iteration of the algorithm we remove a constraint from \( C \), map the pair of nodes \( x \) and \( y \) to their representatives \( u \) and \( v \), and then perform case analysis on the small types of \( u \) and \( v \). In each case we merge the equivalence classes for the two nodes and possibly add more constraints. The main difference from Huet’s algorithm is some special handling of ?s. When we merge two nodes, we need to decide which one to make the representative and thereby decide which label overrides the other. In Huet’s algorithm, a type variable (here nodes labeled var) is overridden by anything else. To handle ?s, we use the rules that ? overrides var but is overridden by anything else. Thus, ? nodes are treated like type variables in that they may merge with any other type. But they are not exactly like type variables in that they override normal type variables. These rules are carried out in cases 3 and 4 of the algorithm.

Before discussing the corner cases of the algorithm (copy_dyn and case 2), we apply the algorithm to the running example introduced in Section 5.1. Figure 9 shows a sequence of snapshots of the solver. Snapshot (a) shows the result of converting the generated constraints to a graph. Constraints are represented as undirected double-lines. At each step, we use bold double-lines to indicate the constraints that are about to be eliminated. To get from (a) to (b) we decompose the constraint between the two function types. Nodes that are no longer the representative of their equivalence class are not shown in the graph. Next we process the two constraints on the left, both of which connect a variable to a function type. The function type becomes the representative in both cases, giving us snapshot (c). As before we decompose a constraint between the two function types into constraints on their children and we have snapshot (d). We first merge the variable node for \( \beta_2 \) into the int node to get (e) and then decompose the constraint between the function type nodes into two more constraints in (f). Here we have constraints on nodes labeled with the ? type. In both cases the node labeled int overrides ? and becomes the representative. The final state is shown in snapshot (g), from which the solutions for the type variables can be read off. As expected, we have \( \alpha = \text{int} \rightarrow \text{int} \).

Case 2 of the algorithm, for \( \alpha \rightarrow v_1 \rightarrow v_2 \), deserves some explanation. Consider the program \((\lambda f : ? . \lambda x : \alpha . f \ x)\). The set of constraints generated from this is \{\( ? \simeq \alpha \rightarrow \beta \)\}. According to the operational semantics from Siek and Taha [29], \( f \) is cast to \( ? \rightarrow ? \), so in some sense, we really should have the constraint \( ? \rightarrow ? \simeq \alpha \rightarrow \beta \). To simulate this in the algorithm we insert two constraints: \( ? \simeq v_1 \) and \( ? \simeq v_2 \). Now, some care must be taken to prevent infinite loops. Consider the constraint \( ? \simeq v \) where \( \text{stype}(v) = v \rightarrow v \). The two new constraints are identical.
solve($C$) =

\[ C := \text{copy\_dyn}(C) \]

for each node $u$ do

\[ u.\text{contains\_vars} := \text{true} \]
end for

while not $C.\text{empty()}$ do

\[ x \simeq y := C.\text{pop()} \]
\[ u := \text{find}(x); v := \text{find}(y) \]

if $u \neq v$ then

\[ (u, v, f) := \text{order}(u, v) \]
\[ \text{union}(u, v, f) \]

\text{case stype}(u) \simeq \text{stype}(v) \text{ of} \]
\[ u_1 \rightarrow u_2 \simeq v_1 \rightarrow v_2 \Rightarrow (* \text{case 1} *) \]
\[ C.\text{push}(u_1, v_1); C.\text{push}(u_2, v_2) \]
\[ | u_1 \rightarrow u_2 \simeq ? \Rightarrow (* \text{case 2} *) \]

if $u.\text{contains\_vars}$ then

\[ u.\text{contains\_vars} := \text{false} \]
\[ w_1 = \text{new\_vertex(stype=?}, \text{contains\_vars=false}) \]
\[ w_2 = \text{new\_vertex(stype=?}, \text{contains\_vars=false}) \]
\[ C.\text{push}(w_1 \simeq u_1); C.\text{push}(w_2 \simeq u_2) \]
\[ | \tau \simeq \text{var} | \tau \simeq ? \Rightarrow (* \text{pass, case 3 and 4} *) \]
\[ | \gamma \simeq \gamma \Rightarrow (* \text{pass, case 5} *) \]
\[ | \_ \Rightarrow \text{error: inconsistent types (* case 6 *)} \]
end while

$G = \text{the quotient of the graph by the equivalence classes}$

if $G$ is acyclic then

\[ \text{return \{u} \mapsto \text{stype(find(u))} \mid \text{u a node in the graph}\} \]
else error

order($u, v$) = \text{case stype}(u) \simeq \text{stype}(v) \text{ of} \]
\[ | ? \simeq \alpha \Rightarrow (u, v, \text{true}) \]
\[ | ? \simeq \tau | \alpha \simeq \tau \Rightarrow (v, u, \text{true}) \]
\[ | \tau \simeq \alpha | \tau \simeq ? \Rightarrow (u, v, \text{true}) \]
\[ | \_ \Rightarrow (u, v, \text{false}) \]

Figure 8: The constraint solving algorithm.
to the original. To avoid this problem we mark each node to indicate whether it may contain a variable. The flags are initialized to true and when we see the constraint $? \simeq v$ we change the flag to false.

The copy dyn function replaces each node labeled $?$ with a new node labeled $\$, thereby removing any sharing of $?$ nodes. This is necessary to allow certain programs to type check, such as the example in Section 3 with the functions $f$, $g$, and $h$. The following is a simplified example that illustrates the same problem.

$$\lambda f : \text{int} \rightarrow \text{bool} \rightarrow \text{int}. \lambda x : ? . f \ x \ x$$

From this program we get the constraint set

$$\{ \text{int} \rightarrow \text{bool} \rightarrow \text{int} \simeq u \_ ? \rightarrow v, \ v \simeq u \_ ? \rightarrow w \}$$

If we forgo the copy dyn conversion and just run the solver, we ultimately get $\text{int} \simeq u \_ ?$ and $\text{bool} \simeq u \_ ?$ which will result in an error. With the copy dyn conversion, the two occurrences of $u \_ ?$ are replaced by separate nodes that can separately unify with int and bool and avoid the error. It is important that we apply the copy dyn conversion to the generated constraints and not to the original program, as that would not avoid the above problem.

The infer function, defined in the following, is the overall inference algorithm, combining constraint generation and solving.

**Definition 4.** (Inference algorithm) Given $\Gamma$ and $e$, let $\tau$, $C$, and $S$ be such that $\Gamma \vdash e : \tau \mid C$ and $S = \text{solve}(C)$. Then $\text{infer}(\Gamma, e) = (S, S(\tau))$.

### 5.3 Properties of the inference algorithm

The substitution $S$ returned from the solver is not idempotent. It can be turned into an idempotent substitution by applying it to itself until a fixed point is reached, which we denote
by $S^*$. Note that the solution $S'$ returned by \texttt{solve} is less or equally informative than the other solutions, thereby avoiding types that would introduce unnecessary cast errors.

**Lemma 4.** (Soundness and completeness of the solver)

1. If $S = \texttt{solve}(C)$ then $S^* \models C$.

2. If $S \models C$ then $\exists S'R$. $S' = \texttt{solve}(C)$ and $R \circ S^* \sqsubseteq S$.

**Proof.** The correctness of the algorithm is based on the following invariant. Let $C$ be the original set of constraints and $C'$ the set of constraints at a given iteration of the algorithm. At each iteration of the algorithm, $S \models C$ if and only if

1. $S \models C'$,

2. for every pair of type variables $\alpha$ and $\beta$ in the same equivalence class, $S(\alpha) = S(\beta)$, and

3. there is an $R$ such that $R \circ S' \sqsubseteq S$, where $S'$ is the current solution based on the stype and union-find data structures.

When the algorithm starts, $C = C'$, so the invariant holds trivially. The invariant is proved to hold at each step by case analysis. Once the algorithm terminates, we read off the answer based on the stype and the union-find data structure. This gives a solution that is less informative but more general (in the Hindley-Milner sense) than any other solution, expressed by the clause $R \circ S^* \sqsubseteq S$.

**Lemma 5.** The time complexity of the \texttt{solve} algorithm is $O(m \alpha(n))$, where $n$ is the number of nodes and $m$ is the number of edges.

**Proof.** The number of iterations in the \texttt{solve} algorithm is $O(m)$. In case 1 of the algorithm we push two constraints into $C$ and make the $v$ node and its two out-edges inaccessible from the \texttt{find} operation. In case 2 of the algorithm, we push two constraints into $C$ and we mark the function type node as no-longer possibly containing variables, which makes it and its two out-edges inaccessible to subsequent applications of case 2. Each iteration performs union-find operations, which have an amortized cost of $\alpha(n)$ [31], so the overall time complexity is $O(m\alpha(n))$.

**Theorem 5.** (Soundness and completeness of inference)

1. If $(S, \tau) = \texttt{infer}(\Gamma, e)$, then $S^*; \Gamma \vdash e : \tau$.

2. If $S; \Gamma \vdash e : \tau$ then there is a $S'$, $\tau'$, and $R$ such that $(S', \tau') = \texttt{infer}(\Gamma, e)$, $R \circ S^* \sqsubseteq S$, and $R \circ S^*(\tau') \sqsubseteq S(\tau)$.

**Proof.** Let $\tau'$ and $C$ be such that $\Gamma \vdash e : \tau'|C$.

1. By the soundness of \texttt{solve} (Lemma 4) we have $S^* \models C$. Then by the equivalence of constraint generation and the type system (Lemma 3), we have $S^*; \Gamma \vdash e : \tau$.

2. By the equivalence of constraint generation and the type system (Lemma 3), we have $S \models C$. Then by the completeness of \texttt{solve} (Lemma 4) there exists $S'$ and $R$ such that $S' = \texttt{solve}(C)$ and $R \circ S^* \sqsubseteq S$. We then conclude using the definition of infer.
Theorem 6. The time complexity of the infer algorithm is $O(n\alpha(n))$ where $n$ is the size of the program.

Proof. The constraint generation step is $O(n)$ and the solver is $O(n\alpha(n))$ (the number of edges in the type graph is bounded by $2n$ because no type has out-degree greater than 2) so the overall time complexity is $O(n\alpha(n))$.

6 Related Work

The interface between dynamic and static typing has been a fertile area of research. We cite a limited number of papers for lack of space. The reader may refer to the references in the cited papers for more detailed lists for each topic.

Optional Types in Dynamic Languages Many dynamic languages allow explicit type annotations. Common LISP [14] is an example. In Common LISP, adding type annotations improves performance but the language does not make the guarantee that annotating all parameters in the program prevents all cast errors at run-time, as is the case for gradual typing. More recently, Tobin-Hochstadt and Felleisen [33, 34] developed a type system for Scheme that facilitates migration between dynamic and static code on a per-module basis.

Type Inference There is a huge body of literature on the topic of type inference, especially regarding variations of the Hindley-Milner type system [17]. Of that, the closest to our work is that on combining inference and subtyping [4, 26]. The main difference between inference for subtyping versus gradual typing is that subtyping has co/contra-variance in function types, whereas the consistency relation is covariant in both the parameter and return type, making the inference problem for gradual typing more tractable.

Gradual Typing In addition to the related work discussed in the introduction, we mention a couple more related works here. Anderson and Drossopoulou developed a gradual type system for BabyJ [2] that uses nominal types. Gronski, Knowles, Tomb, Freund, and Flanagan [9] provide gradual typing in the Sage language by including a dynamic type and implicit down-casts. They use a modified form of subtyping to provide the implicit down-casts.

Quasi-static Typing Thatte’s Quasi-Static Typing [32] is close to gradual typing but relies on subtyping and treats the unknown type as the top of the subtype hierarchy. Siek and Taha [29] show that implicit down-casts combined with the transitivity of subtyping creates a fundamental problem that prevents this type system from catching all type errors even when all parameters in the program are annotated.

Soft Typing Static analyses based on dataflow can be used to perform static checking and to optimize performance. The later variant of Soft Typing by Flanagan and Felleisen [7] is an example of this approach. These analyses provide warnings to the programmer while still allowing the programmer to execute their program immediately (even programs with errors), thereby preserving the benefits of dynamic typing. However, the programmer does not control which portions of a program are statically checked: these whole-program analyses have non-local interactions.

Dynamic Typing in Statically Typed Languages Abadi et al. [1] extended a statically typed language with a Dynamic type and explicit injection (dynamic) and projection operations (typecase). Their approach does not satisfy the goals of gradual typing, as migrating code between dynamic and static checking not only requires changing type annotations on parameters, but also adding or removing injection and projection operations throughout the code. Gradual typing automates the latter.

Hybrid Typing The Hybrid Type Checking of Flanagan [5] combines standard static typing with refinement types, where the refinements may express arbitrary predicates. This is
analogous to gradual typing in that it combines a weaker and stronger type system, allowing implicit coercions between the two systems and inserting run-time checks. A notable difference is that hybrid typing is based on subtyping whereas gradual typing is based on type consistency.

7 Conclusion

This paper develops a type system for the gradually typed lambda calculus with type variables \( \lambda^? \alpha \). The system integrates type inference and gradual typing to aid programmers in adding types to their programs. In the proposed system, a programmer uses a type variable annotation to request the best solution for the variable from the inference algorithm.

The type system presented satisfies the defining properties of a gradual type system. That is, a programmer may omit type annotations on function parameters and immediately run the program; run-time type checks are performed to preserve type safety. Furthermore, a programmer may add type annotations to increase static checking. When all function parameters are annotated, all type errors are caught at compile-time.

The paper also develops an efficient inference algorithm for \( \lambda^? \alpha \) that is sound and complete with respect to the type system and that takes care not to infer types that would introduce cast errors.

A Isabelle Formalization

A.1 Syntax and Auxiliary Functions

\textbf{types} \ name = nat

\textbf{datatype} ty =
\begin{align*}
U\text{VarT} & \text{name} \\
\text{IntT} & \text{(int)} \\
\text{BoolT} & \text{(bool)} \\
\text{DynT} & \text{(\( ? \))} \\
\text{ArrowT} & \text{ty ty} \text{ (infixr \( \to \))}
\end{align*}

\textbf{datatype} const = \text{IntC} \text{ int} \\
\text{BoolC} \text{ bool} \\
\text{Succ} \\
\text{IsZero}

\textbf{datatype} expr =
\begin{align*}
\text{Var} & \text{ name} \\
\text{Const} & \text{ const} \\
\text{Lam} & \text{name ty expr} \text{ (\( \lambda -: - \))} \\
\text{App} & \text{expr expr}
\end{align*}

\textbf{types} env = \text{(name \( \times \) ty) list} \\
\textbf{types} subst = \text{(name \( \times \) ty) list}

\textbf{axclass} type-struct < type

\textbf{instance} ty::type-struct ..
\textbf{instance} expr::type-struct ..
\textbf{instance} nat::type-struct ..
\textbf{instance} option::(type-struct)type-struct ..
instance fun::(type, type-struct)type-struct ..
instance list::(type-struct)type-struct ..
instance set::(type-struct)type-struct ..
instance *::(type-struct,type-struct)type-struct ..

A.1.1 Auxilliary Functions

constdefs id-subst :: subst
  id-subst-def[simp]: id-subst ≡ []
— domain of an association list

consts
  Dom :: ('a × 'b) list ⇒ 'a set
primrec
  Dom [] = {}
  Dom (xt#ls) = insert (fst xt) (Dom ls)

consts
  lookup :: ('a × 'b) list ⇒ 'a ⇒ 'b option
primrec
  lookup [] k = None
  lookup (kv#ls) k =
    (if fst kv = k then Some (snd kv) else lookup ls k)

constdefs
  lookup-subst :: (name × ty) list ⇒ name ⇒ ty (%)
  lookup-subst S a ≡
    (case (lookup S a) of None ⇒ UVarT a |
         Some t ⇒ t)

consts
  app-subst :: [subst, 'a::type-struct] ⇒ 'a::type-struct ($)
syntax (latex)
  app-subst :: [subst, 'a::type-struct] ⇒ 'a::type-struct ()

primrec (app-subst-ty)
  $S (UVarT a) = % S a
  $S (IntT) = (IntT)
  $S (BoolT) = (BoolT)
  subst-fun: $S (t1 → t2) = ($S t1) → ($S t2)
  $S (? ) = (? )

primrec (app-subst-list)
  $S [] = []
  $S (x#xs) = ($S x)#($S xs)

defs (overloaded)
  app-subst-pair: $S p ≡ (fst p, $S (snd p))

primrec (app-subst-expr)
  subst-var: $S (Var x) = (Var x)
  $S (Const c) = (Const c)
  subst-abs: $S (λx::r. e) = (λx:$S r. $S e)
  $S (App e1 e2) = (App ($S e1) ($S e2))

primrec (app-subst-option)
  app-subst S None = None

23
app-subst $S$ (Some $\tau$) = Some (app-subst $S$ $\tau$)

defs (overloaded)
app-subst-fun: app-subst $S$ $\Gamma$ $\equiv$ ($\lambda$ $x$. app-subst $S$ ($\Gamma$ $x$))

consts $FTV :: \text{'a::type-struct} \Rightarrow \text{nat set}$

primrec (FTV-ty)
$FTV$ ($\text{UVarT} \alpha$) = $\{\alpha\}$
$FTV$ ($\text{IntT}$) = $\{\}$
$FTV$ ($\text{BoolT}$) = $\{\}$
$FTV$ ($\text{DynT}$) = $\{\}$
$FTV$ ($t1 \rightarrow t2$) = $FTV$ $t1$ $\cup$ $FTV$ $t2$

primrec (FTV-exp)
$FTV$ ($Var$ $x$) = $\{\}$
$FTV$ ($Const$ $c$) = $\{\}$
$FTV$ ($\lambda$ $x$:$\tau$. $e$) = $FTV$ $\tau$ $\cup$ $FTV$ $e$
$FTV$ ($\text{App}$ $e1$ $e2$) = $FTV$ $e1$ $\cup$ $FTV$ $e2$

primrec (FTV-option)
$FTV$ $\text{None}$ = $\{\}$
$FTV$ ($\text{Some} \tau$) = $FTV$ $\tau$

primrec (FTV-list)
$FTV$ $[]$ = $\{\}$
$FTV$ ($a$#$\text{ls}$) = $FTV$ $a$ $\cup$ $FTV$ $\text{ls}$

defs (overloaded)
$FTV$-nat[simp]: $FTV$ $x$ $\equiv$ $\{x\}$

defs (overloaded)
$FTV$-pair[simp]: $FTV$ $p$ $\equiv$ $FTV$ ($\text{snd}$ $p$)

defs (overloaded)
$FTV$-set: $FTV$ $C$ $\equiv$ $\{\alpha . \exists$ $e$. $\alpha$ $\in$ $FTV$ $e$ $\land$ $e$ $\in$ $C\}$

defs (overloaded)
$FTV$-fun: $FTV$ $\Gamma$ $\equiv$ $\{\alpha . \exists$ $y$ $t$. $\Gamma$ $y$ $=$ $t$ $\land$ $\alpha$ $\in$ $FTV$ $t\}$

consts $\text{no-dyn :: 'a::type-struct} \Rightarrow \text{bool}$

primrec (no-dyn-ty)
$\text{no-dyn}$ ($\text{UVarT} \alpha$) = $\text{True}$
$\text{no-dyn}$ ($\text{IntT}$) = $\text{True}$
$\text{no-dyn}$ ($\text{BoolT}$) = $\text{True}$
$\text{no-dyn}$ ($\text{DynT}$) = $\text{False}$
$\text{no-dyn}$ ($t1 \rightarrow t2$) = (if $\text{no-dyn}$ $t1$ then $\text{no-dyn}$ $t2$ else $\text{False}$)

primrec (no-dyn-exp)
$\text{no-dyn}$ ($Var$ $x$) = $\text{True}$
$\text{no-dyn}$ ($Const$ $c$) = $\text{True}$
$\text{no-dyn}$ ($\lambda$ $x$:$\tau$. $e$) = (if $\text{no-dyn}$ $\tau$ then $\text{no-dyn}$ $e$ else $\text{False}$)
$\text{no-dyn}$ ($\text{App}$ $e1$ $e2$) = (if $\text{no-dyn}$ $e1$ then $\text{no-dyn}$ $e2$ else $\text{False}$)
defs (overloaded)
  no-dyn-fun: no-dyn Γ ≡ (∀ x a. Γ x = a → no-dyn a)

primrec (no-dyn-option)
  no-dyn None = True
  no-dyn (Some τ) = no-dyn τ

defs (overloaded)
  no-dyn-pair[simp]: no-dyn p ≡ no-dyn (snd p)

primrec (no-dyn-list)
  no-dyn [] = True
  no-dyn (a#ls) = (if no-dyn a then no-dyn ls else False)

constdefs idempotent :: subst ⇒ bool
  idempotent S ≡ $S (S t) = $S t

A.1.2 Properties of Auxiliary Functions

lemma finite-ftv-ty[intro!]: finite (FTV (τ::ty))
  apply (induct τ) by auto

lemma finite-ftv-expr[intro!]: finite (FTV (e::expr))
  apply (induct e) by auto

lemma finite-ftv-subst[intro!]: finite (FTV (S::subst))
  apply (induct S) by auto

lemma id-id[simp]: $id-subst (τ::ty) = τ apply (induct τ)
  using lookup-subst-def by auto

lemma closed-subst-id: FTV τ = {} ⇒ $S τ = (τ::ty)
  apply (induct τ) by auto

lemma idempotent-ty[rule-format]:
  ∀ S. idempotent S → $S ($S t) = $S (t::ty)
  apply (induct t) defer apply simp apply simp apply simp apply simp
  proof
  fix n::nat
  show ∀ S. idempotent S → $S ($S (UVarT n)) = $S (UVarT n)
  proof clarify
    fix S assume id: idempotent S
    have $S ($S (UVarT n)) = $S (%S n) by simp
    also have ... = ($S (%S) ) n by (simp add: app-subst-fun)
    also from id have ... = %S n by (simp add: idempotent-def)
    also have ... = $S (UVarT n) by simp
    finally show $S ($S (UVarT n)) = $S (UVarT n) by blast
  qed

lemma ftv-dom-id[rule-format]:
  ∀ S. (∀ a. a ∈ FTV τ → % S a = UVarT a) = ($S τ = (τ::ty))
  apply (induct τ) by auto

  — This is Lemma 2 of the paper

lemma t1tot2eqSt-implies-t2eqSt2[rule-format]:
idempotent $S \land (S \tau \Rightarrow \tau_1 \Rightarrow \tau_2) \Rightarrow \tau_2 = S \tau_2$  

apply (induct-tac $\tau$) defer apply force apply force apply force apply force 
apply simp apply (rule impI) defer apply (rule impI)

proof –
fix $a$
assume tmp: idempotent $S \land S (UVarT a) = \tau_1 \Rightarrow \tau_2$
from tmp have idems: idempotent $S$ by simp
from idems have sstt: $S (S (UVarT a)) = (S (S (UVarT a)))$
by (rule idempotent-ty)
with tmp sstt have sneqst1tost2: $(S (UVarT a)) = S \tau_1 \Rightarrow S \tau_2$ by simp
with tmp show $\tau_2 = S \tau_2$ by simp

next
fix $ty1 ty2$
assume styc: idempotent $S \land S ty1 = \tau_1 \land S ty2 = \tau_2$

hence idempotent $S$ by simp
hence $S (S ty2) = S ty2$ by (rule idempotent-ty)
with styc show $\tau_2 = S \tau_2$ by simp

qed

lemma Steqt1tot2-implies-t2eqSt2[rule-format]:

$idempotent S \land (\tau_1 \Rightarrow \tau_2 = S \tau) \Rightarrow \tau_2 = S \tau_2$

proof –

have idempotent $S \land S \tau = \tau_1 \Rightarrow \tau_2 \Rightarrow \tau_2 = S \tau_2$

using t1tot2eqSt-implies-t2eqSt2 by blast
thus idempotent $S \land (\tau_1 \Rightarrow \tau_2 = S \tau) \Rightarrow \tau_2 = S \tau_2$ by auto

qed

lemma Steqt1tot2-implies-st2eqt2:

\[ \text{idempotent } S; \tau_1 \Rightarrow \tau_2 = S \tau \implies S \tau_2 = \tau_2 \]
using Steqt1tot2-implies-t2eqSt2 by auto

A.2 The Simply Typed Lambda Calculus

consts $\text{TypeOf} :: \text{const} \Rightarrow ty$

primrec
$\text{TypeOf} (\text{IntC } n) = \text{IntT}$
$\text{TypeOf} (\text{BoolC } b) = \text{BoolT}$
$\text{TypeOf } \text{Succ} = \text{IntT} \Rightarrow \text{IntT}$
$\text{TypeOf } \text{IsZ0} = \text{IntT} \Rightarrow \text{BoolT}$

inductive stlc-wt :: $\text{env} \Rightarrow \text{expr} \Rightarrow ty \Rightarrow \text{bool}$ ($\vdash - \cdot : - [52,52,52,52]$ 51)

where
Var[intro!]: \[ \text{lookup } \Gamma \cdot x = \text{Some } \tau \] $\Rightarrow \Gamma \vdash \text{Var } x : \tau$

Abs[intro!]: \[ (x, \tau_1) \# \Gamma \vdash e : \tau_2 \] $\Rightarrow \Gamma \vdash (\lambda x : \tau_1. \ e) : \tau_1 \Rightarrow \tau_2$

App[intro!]: \[ \Gamma \vdash e : \tau_1 \Rightarrow \tau_2; \Gamma \vdash e' : \tau_1 \] $\Rightarrow \Gamma \vdash (\text{App } e \ e') : \tau_2$

inductive stlc-wt :: [:subst,env] $\Rightarrow$ [expr,ty] $\Rightarrow$ bool ($\vdash - \cdot : - [52,52,52,52]$ 51)

where
SVar[intro!]: \[ \text{lookup } \Gamma \cdot x = \text{Some } \tau \] $\Rightarrow S; \Gamma \vdash \text{Var } x : \tau$

SConst[intro!]: \[ \tau = \text{TypeOf } c \Rightarrow S; \Gamma \vdash \text{Const } c : \tau \]

SAbs[intro!]: \[ S ; (x, \tau_1) \# \Gamma \vdash e : \tau_2 \] $\Rightarrow S; \Gamma \vdash (\lambda x : \tau_1. \ e) : \tau_1 \Rightarrow \tau_2$
proof

lemma \textit{ex-t[rule-format]}: \forall S x. lookup ($S$::\textit{subst}) $\Gamma$::\textit{env} $x = \text{Some } \tau \longrightarrow

(\exists \tau'. \text{ lookup } \Gamma \cdot x = \text{Some } \tau' \land \forall S \tau' = \tau)

apply (induct $\Gamma$)

apply simp

apply clarify apply (simp add: \textit{app-subst-pair})

apply (case-tac $a = x$) apply simp

apply auto

done

lemma \textit{idem-ftvst-impl}:

\forall S a. \text{ idempotent } S \land a \in \text{FTV} ($S$ ($\tau::\textit{ty}$)) \longrightarrow \%S a = \text{UVarT} a

apply (induct $\tau$)

deferd apply simp apply simp apply simp apply simp apply simp apply blast

apply clarify

proof –

fix $b\ S\ a$

assume ids: \text{ idempotent } S \land a \in \text{FTV} ($S$ ($\text{UVarT} \ b$))

from ids have \%S ($S$ ($\text{UVarT} \ b$)) = \%S ($\text{UVarT} \ b$) by (rule \textit{idempotent-ty})

hence \forall a. a \in \text{FTV} ($S$ ($\text{UVarT} \ b$)) \longrightarrow \%S a = \text{UVarT} a using \textit{ftv-dom-id} by blast

with \textit{after} show \%S a = \text{UVarT} a by simp

qed

lemma \textit{idem-ftvst}:

\[ \forall S a \in \text{FTV} ($S$ ($\tau::\textit{ty}$)) \Longrightarrow \%S a = \text{UVarT} a \]

using \textit{idem-ftvst-impl} by blast

lemma \textit{ftv-wt-sub-impl}: $\Gamma' \vdash e' : \tau \longrightarrow

\forall \Gamma.e S. \text{ idempotent } S \land \Gamma' = \%S \Gamma \land e' = \%S e

\longrightarrow (\forall a. a \in \text{FTV} \tau \longrightarrow \%S a = \text{UVarT} a)

apply (induct rule: \textit{stlc-wt inducing})

deferd apply (case-tac $c$)

apply force apply force apply force apply force apply force apply force apply force prefer 2

apply clarify apply (case-tac $ea$) apply force apply force apply force prefer 2

apply clarify apply (\textit{rule} $\text{expr}$ $x=x\cdot\tau_1$) apply \%$\Gamma$ in \textit{allE}

apply (\textit{rule} $\text{expr}$ $x=x\cdot\tau_1$) apply \%$\Gamma$ in \textit{allE}

apply (\textit{rule} $\text{expr}$ $x=x\cdot\tau_1$) apply \%$\Gamma$ in \textit{allE}

apply (\textit{rule} $\text{expr}$ $x=x\cdot\tau_1$) apply \%$\Gamma$ in \textit{allE}

apply (\textit{rule} $\text{expr}$ $x=x\cdot\tau_1$) apply \%$\Gamma$ in \textit{allE}

apply (\textit{rule} $\text{expr}$ $x=x\cdot\tau_1$) apply \%$\Gamma$ in \textit{allE}

apply (\textit{rule} $\text{expr}$ $x=x\cdot\tau_1$) apply \%$\Gamma$ in \textit{allE}

apply clarify apply (\textit{rule} $\text{expr}$ $x=x\cdot\tau_1$) apply \%$\Gamma$ in \textit{allE}

apply clarify apply (\textit{rule} $\text{expr}$ $x=x\cdot\tau_1$) apply \%$\Gamma$ in \textit{allE}

apply clarify apply (\textit{rule} $\text{expr}$ $x=x\cdot\tau_1$) apply \%$\Gamma$ in \textit{allE}

apply clarify apply (\textit{rule} $\text{expr}$ $x=x\cdot\tau_1$) apply \%$\Gamma$ in \textit{allE}

apply clarify apply (\textit{rule} $\text{expr}$ $x=x\cdot\tau_1$) apply \%$\Gamma$ in \textit{allE}

apply clarify apply (\textit{rule} $\text{expr}$ $x=x\cdot\tau_1$) apply \%$\Gamma$ in \textit{allE}

apply clarify apply (\textit{rule} $\text{expr}$ $x=x\cdot\tau_1$) apply \%$\Gamma$ in \textit{allE}

apply clarify apply (\textit{rule} $\text{expr}$ $x=x\cdot\tau_1$) apply \%$\Gamma$ in \textit{allE}

apply clarify

proof –

fix $\Gamma\ x$ and $\tau::\textit{ty}$ and $\Gamma'\ e$ and $S::\textit{subst}$ and $a$

assume \textit{sgx}: lookup ($S$ $\Gamma$) $x = \text{Some } \tau$ and \textit{ids}: \text{ idempotent } S

and \textit{xxe}: \text{Var } x = \%S e \land \textit{aft}: a \in \text{FTV} \tau

from \textit{sgx} have $X$: $\exists \tau'$. lookup $\Gamma'\ x = \text{Some } \tau'$ \land $\forall S \tau' = \tau$ by (rule \textit{ex-t})

from $X$ obtain $\tau'$ where \textit{gpx}: lookup $\Gamma'\ x = \text{Some } \tau'$ and \textit{stp}: \%$S \tau' = \tau$ by blast
from aft stp have afst: $a \in FTV (\$S \, \tau')$ by simp
from ids afst show $\% S \ a = UVarT \ a$ by (rule idem-ftvst)
qed

lemma ftv-wt-sub: [$S \Gamma \vdash S \ e : \tau$; idempotent $S$]  
$\implies (\forall \ a \ . \ a \in FTV \ \tau \implies \%S \ a = UVarT \ a)$
using ftv-wt-sub-impl apply blast done

— Lemma 1 of the paper

lemma ewt-steqSt:
assumes idem: idempotent $S$ and ewt: $S \Gamma \vdash S \ e : \tau$
shows $S \tau = \tau$
using idem ewt ftv-wt-sub ftv-dom-id by blast

lemma ewt-ewSt:
assumes idem: idempotent $S$ and ewt: $S \Gamma \vdash S \ e : \tau$
shows $S \Gamma \vdash S \ e : S \tau$
proof -
from ewt idem have $(\forall \ a \ . \ a \in FTV \ \tau \implies \%S \ a = UVarT \ a)$ by (rule ftv-wt-sub)
  hence $S \tau = \tau$ using ftv-dom-id by blast
  thus $S \Gamma \vdash S \ e : S \tau$ by simp
qed

lemma ewt-teqSt:
assumes idem: idempotent $S$ and ewt: $S \Gamma \vdash S \ e : \tau$
shows $\tau = S \tau$
proof -
from idem ewt have $S \tau = \tau$ by (rule ewt-steq)
  thus $\tau = S \tau$ by auto
qed

lemma stlc-implies-istlc-impl:
$\Gamma \vdash e' : \tau' \implies$
$(\forall \ \Gamma \ e \ S \ \tau . \ idempotent \ S \wedge \Gamma' = \%S \ a = UVarT \ a)$
$\implies (\exists \ \tau'' . \ (S;\Gamma \vdash e : \tau'' \wedge \%S \ \tau'' = \tau'))$
apply (induct rule: stlc-wt.induct)
apply clarify defer apply clarify defer apply clarify defer apply clarify defer
proof -
fix $\Gamma \ x \ \tau$ and $\Gamma'::ew$ and $e::expr$ and $S::sub$t and $\tau'$
assume $\exists gx: lookup (\%S \Gamma') x = Some (\%S \ \tau')$ and idem: idempotent $S$
and $\exists vx: Var \ x = S \ e$
from $\exists gx \ ex-t$ obtain $\tau''$ where $lxg: lookup \Gamma' x = Some \ \tau''$
and $\exists stt: S \ \tau'' = S \ \tau'$ by blast
from $\exists vx \ lxx \ stst \ show \ \exists \tau'' . \ (S;\Gamma' \vdash e : \tau'' \wedge \%S \ \tau'' = \tau )$
apply (case-tac $e::expr$) apply (rule-tac $x=\tau''$ in exI) by auto
next
fix $\Gamma \ c \ \Gamma' \ e \ S \ \tau$
assume idem: idempotent $S$ and Const $c = S \ e$ and $TypeOf \ c = S \ \tau$
thus $\exists \tau'' . \ (S;\Gamma' \vdash e : \tau'' \wedge \%S \ \tau'' = TypeOf \ c)$
apply (rule-tac $x=TypeOf \ c$ in exI)
apply (simp add: idempotent-ty)
apply (case-tac $e::expr$) apply auto done
next
fix $\tau_1 \Gamma e \ \tau_2 \Gamma' \ ea \ S \ \tau$
assume $IH1: \forall \Gamma \ ea \ S \ \tau$. 

28
idempotent $Sa \wedge$
\[(x, \tau_1) \# S \Gamma' = S \Gamma \wedge e = S \Gamma \wedge \tau_2 = S \Gamma \Gamma \rightarrow \]
$(\exists \tau'' : S \Gamma \Gamma \Gamma \vdash \tau' \wedge S \Gamma \Gamma \Gamma \tau'' = \tau_2)$
\[\text{and ids: idempotent $S$ and le: } \lambda x: \tau_1, e = S \Gamma \varepsilon \text{ and } t12st: \tau_1 \vdash \tau_2 = S \Gamma \varepsilon \]
\[\text{from le obtain } t b \text{ where } ea : \lambda x : t. b \text{ and } t1st: \tau_1 = S \Gamma t \]
\[\text{and esb: } e = S b \text{ apply (case-tac ea::expr) apply auto done} \]
from ids $t12st$ have $t2st2: \tau_2 = S \Gamma \varepsilon \tau_2 \text{ using Steq11t3-implies-12eqSt2 by blast} \]
from $e a \text{ IH1 t1st} \varepsilon e \text{ esb}
have $X : \exists \tau''. S \Gamma' \vDash b : \tau'' \wedge S \Gamma \varepsilon \tau_2$
apply auto apply (erule-tac $x = x, t) \# \Gamma' \in \text{allE} \)
\[\text{apply (erule-tac } x = b \text{ in allE)} \]
\[\text{apply (erule-tac } x = S \text{ in allE)} \]
\[\text{apply (erule-tac } x = \tau_2 \text{ in allE) apply auto} \]
\[\text{apply (simp add: app-subst-pair) using } t2st2 \text{ apply simp done} \]
from $X \text{ obtain } t2 \text{ where } wt : S. t(x, t) \# \Gamma' = b : t2 \text{ and } st2t2 : S t2 = \tau_2 \text{ by blast} \]
from $wt b \text{ have wt1: } S \Gamma' \vDash \lambda x : t. b : t \rightarrow t2 \text{ by blast} \]
with $e a \text{ st2t2 t1st}$
show $\exists \tau''. S \Gamma' \vDash \tau : \tau'' \wedge S \Gamma \varepsilon \tau = \tau_1 \rightarrow \tau_2 \text{ by auto} \]
next
\[\text{fix } \Gamma e \tau_1 \tau_2 \epsilon' \Gamma' \varepsilon \text{ esb } S \tau \]
assume $wte: S \Gamma' \vDash e : \tau_1 \rightarrow S \Gamma \varepsilon \tau$
\[\text{and IH1: } \forall \Gamma e \text{ Sa } \tau'. \]
idempotent $Sa \wedge$
\[S \Gamma' = S \Gamma \wedge e = S \Gamma \wedge \tau_1 \rightarrow S \Gamma \varepsilon \tau \rightarrow (\exists \tau'' : S \Gamma \Gamma \varepsilon \Gamma \Gamma \Gamma \vdash \tau'' \wedge S \Gamma \Gamma \Gamma \tau'' = \tau_1) \]
\[\text{and wtep: } S \Gamma' \vDash \epsilon' : \tau_1 \]
\[\text{and IH2: } \forall \Gamma e \text{ Sa } \tau. \]
idempotent $Sa \wedge S \Gamma = S \Gamma \wedge e = S \Gamma \wedge \tau_1 = S \Gamma \tau \rightarrow (\exists \tau'' : S \Gamma \Gamma \varepsilon \Gamma \Gamma \Gamma \vdash \tau'' \wedge S \Gamma \Gamma \Gamma \tau'' = \tau_1) \]
\[\text{and ids: idempotent } S \text{ and } A: \text{ App } e \epsilon' = S \varepsilon e \]
\[\text{from } A \text{ obtain } e1 e2 \text{ where } EA: \text{ e1 = App } e1 e2 \text{ and } E: e = S \Gamma e1 \]
\[\text{and EP: } e' = S S e2 \text{ apply (case-tac ea::expr) by auto} \]
\[\text{from ids wte E have } \tau_1 = S \Gamma \varepsilon \tau \rightarrow S \Gamma \varepsilon \tau = S (\tau_1 \rightarrow S \Gamma \varepsilon \tau) \text{ using ewt-teqSt by blast} \]
hence $t1st1: \tau_1 = S \Gamma \varepsilon \tau_1 \text{ by simp} \]

from $e a \text{ IH1 t1st1} \text{ obtain } t1 \text{ where } wte1: S \Gamma' \vDash e1 : t1 \]
\[\text{and st1tst: } S t1 = t1 \rightarrow S \Gamma \varepsilon \tau \]
\[\text{apply auto apply (erule-tac } x = \Gamma' \in \text{allE} \)
\[\text{apply (erule-tac } x = e1 \text{ in allE)} \]
\[\text{apply (erule-tac } x = S \text{ in allE)} \]
\[\text{apply (erule-tac } x = \tau_1 \text{ in allE)} \]
\[\text{apply auto using idempotent-ty apply simp done} \]
from $e a \text{ EP IH2} \text{ obtain } t2 \text{ where } wte2: S \Gamma' \vDash e2 : t2 \text{ and } st2t1: S t2 = \tau_1 \]
\[\text{apply simp apply (erule-tac } x = \Gamma' \in \text{allE} \)
\[\text{apply (erule-tac } x = e2 \text{ in allE)} \]
\[\text{apply (erule-tac } x = S \text{ in allE)} \]
\[\text{apply (erule-tac } x = \tau_1 \text{ in allE)} \]
\[\text{apply auto using t1st1 apply simp done} \]
from st1tst st2t1 have eq: $S t1 = S t2 = \tau \text{ by simp} \]
from $wte1 wte2 eq \text{ EA}$
show $\exists \tau'': S \Gamma' \vDash \tau : \tau'' \wedge S \Gamma \varepsilon \tau'' = S \Gamma \varepsilon \tau \text{ by auto} \]
qed

lemma stlc-implies-istlc-impl2:
\[\text{idempotent } S : S \Gamma \Gamma \vDash S \varepsilon e : S \Gamma \varepsilon \tau \implies \exists \tau'. S \Gamma \Gamma \Gamma \vdash \tau' \wedge S \Gamma \Gamma \Gamma \tau' = S \Gamma \varepsilon \tau \]
using stlc-implies-istlc-impl by blast
lemma stlc-implies-istlc:
    assumes wte: $S \Gamma \vdash S e : \tau$ and ids: idempotent $S$
    shows $\exists \tau'. S;\Gamma \vdash e : \tau' \land S \tau' = \tau$
proof
    from ids wte have ute2: $S \Gamma \vdash S e : S \tau$ by (rule wte-ewSt)
    from ids wte2 obtain $\tau'$ where wtep: $S;\Gamma \vdash e : \tau'$ and stst: $S \tau' = S \tau$
    using stlc-implies-istlc-impl2 by blast
    from ids wte have $S \tau = S \tau$ by (rule wte-ewSt)
    with wtep stst show ?thesis by auto
qed

lemma stlc-wt-implies-teqSt:
    assumes idsms: idempotent $S$ and ids: $S \Gamma \vdash S e : \tau$
    shows $\tau = S \tau$
proof
    from wte idsms have $\forall a. a \in FTV \tau \longrightarrow \%a = UVarT a$ by (rule ftv-wt-sub)
    hence $S \tau = S \tau$ using ftv-dom-id by blast
    thus $\tau = S \tau$ by auto
qed

lemma subst-const[simp]: $S (TypeOf c) = TypeOf c$
    apply (case-tac c) apply auto done

lemma subst-env[rule-format]:
    $\forall x \tau S. \text{lookup } \Gamma x = \text{Some } \tau \longrightarrow \text{lookup } (S \Gamma) x = \text{Some } (S \tau)$
    apply (induct $\Gamma$) apply simp
    apply clarify apply (simp add: app-subst-pair)
    apply (case-tac a = x) apply simp
    apply auto
    done

lemma istlc-implies-stlc:
    $S;\Gamma \vdash e : \tau \Longrightarrow S;\Gamma \vdash S e : S \tau$
    apply (induct rule: istlc-wt.induct)
    apply simp apply (rule Var) apply (simp add: subst-env)
    apply simp apply blast
defer
    apply simp apply (rule App) apply simp apply simp
proof
    fix $S$ and $\Gamma$::env and $\tau_1, \tau_2 \in e$
    assume $S; (x,\tau_1) \# \Gamma \vdash e : \tau_2$ and SE: $S (x,\tau_1) \# \Gamma \vdash S e : S \tau_2$
    have $S (x,\tau_1) \# \Gamma = (x, S \tau_1) \# (S \Gamma)$ by (simp add: app-subst-pair)
    with SE have $(x, S \tau_1) \# (S \Gamma) \vdash S e : S \tau_2$ by simp
    thus $S;\Gamma \vdash S (\lambda x: \tau_1. e) : S (\tau_1 \rightarrow \tau_2)$ by auto
qed

— Theorem 1 of the paper

theorem stlc-istlc-equivalent:
    (idempotent $S$ ∧ $S \Gamma \vdash S e : \tau$ → ($\exists \tau'. S;\Gamma \vdash e : \tau' \land S \tau' = \tau$))
    ∧ ($S;\Gamma \vdash e : \tau$ → $S;\Gamma \vdash S e : S \tau$)
    apply (rule conjI)
    using stlc-implies-istlc apply simp
    using istlc-implies-stlc apply simp
done
A.3 Choosing Fresh Variables

In various places within the formal development we need to choose a “fresh” variable. More specifically, we need to choose a variable that is not in some set, such as the domain of the type environment. Variables are represented here as natural numbers, and we constructively choose a fresh variable by taking the successor of the maximum number in the set. Of course, we must assume that the set in question is finite.

```
constdefs max :: nat ⇒ nat ⇒ nat
max x y ≡ (if x < y then y else x)
declare max-def [simp]
```

To define the maximum number in a set, we take advantage of Isabelle’s ability to fold over a finite set. To use fold with the above max function, we must first prove a few properties of max, but the proofs go through automatically.

```
interpretation AC-max: ACe [max 0 :: nat]
  by (unfold-locales (auto intro: add-assoc add-commute))
```

```
constdefs setmax :: nat set ⇒ nat
setmax S ≡ fold max (λx. x) 0 S
```

We want to show that the successor of the maximum element of a set is not in the set. Towards proving that we prove the following lemma.

```
lemma max-ge: finite L ⇒ ∀x∈L. x ≤ setmax L
  apply (induct rule: finite-induct)
  apply simp
  apply clarify
  apply (case-tac xa = x)
  proof
    fix x and F::nat set and xa
    assume fF: finite F and xF: x ∉ F and xax: xa = x
    from fF xF have mc: setmax (insert x F) = max x (setmax F)
      apply (simp only: setmax-def)
      apply (rule AC-max.fold-insert)
      apply auto done
    with xax show xa ≤ setmax (insert x F)
      apply clarify by simp
  next
    fix x and F::nat set and xa
    assume fF: finite F and xF: x ∉ F
      and axF: ∀x∈F. x ≤ setmax F
    and zxF: xa ∈ insert x F
    and xax: xa ≠ x
    from xax zxF have xaF: xa ∈ F by auto
    with axF have xasF: xa ≤ setmax F by blast
    from fF xF have mc: setmax (insert x F) = max x (setmax F)
      apply (simp only: setmax-def)
      apply (rule AC-max.fold-insert)
      apply auto done
    with xasF show xa ≤ setmax (insert x F) by auto
  qed
```

```
lemma max-is-fresh[simp]:
```
assumes $F$: finite $L$ shows $\text{Suc (setmax } L) \notin L$

proof
  assume ssl: $\text{Suc (setmax } L) \in L$
  with $F$ max-ge have $\text{Suc (setmax } L) \leq \text{setmax } L$ by blast
  thus False by simp
qed

lemma greater-than-max-is-fresh[simp]:
  assumes $F$: finite $L$ and $I$: $\text{setmax } L < i$
  shows $i \notin L$

proof
  assume ssl: $i \in L$
  with $F$ max-ge have $i \leq \text{setmax } L$ by blast
  with $I$ show False by simp
qed

lemma subset-implies-lessmax-impl:
  finite $A$ = $\Rightarrow \forall B$. finite $B$ $\wedge$ $A \subseteq B$ $\rightarrow$ $\text{setmax } A \leq \text{setmax } B$

apply (induct rule:finite-induct)
apply (simp add: setmax-def)
proof
  fix $x F$ assume $fF$: finite $F$ and $xF$: $x \notin F$
  and IH: $\forall B$. finite $B$ $\wedge$ $F \subseteq B$ $\rightarrow$ $\text{setmax } F \leq \text{setmax } B$
  show $\forall B$. finite $B$ $\wedge$ insert $x F \subseteq B$ $\rightarrow$ $\text{setmax } (\text{insert } x F) \leq \text{setmax } B$
    proof clarify
      fix $B$ assume $fB$: finite $B$ and $xFsubB$: insert $x F \subseteq B$
      from $fF$ $xF$ have $\text{smxF}: \text{setmax } (\text{insert } x F) = \text{max } x \ (\text{setmax } F)$
      apply (simp only: setmax-def) apply (rule AC-max.fold-insert) by auto
      from $xFsubB$ have $xB$: $x \in B$ by auto
      from $fB$ $xB$ have $\text{zleB}: x \leq \text{setmax } B$ using max-ge by blast
      from $fB$ $xFsubB$ have $\text{FsubB}: F \subseteq B$ by auto
      from $fB$ $\text{FsubB}$ IH have $\text{setmax } F \leq \text{setmax } B$ by simp
      with $\text{zleB smxF}$ show $\text{setmax } (\text{insert } x F) \leq \text{setmax } B$ by simp
    qed
qed

lemma subset-implies-lessmax:
  [$ [\text{finite } B; A \subseteq B ] \Rightarrow \text{setmax } A \leq \text{setmax } B $]

apply (frule finite-subset) apply simp
using subset-implies-lessmax-impl apply simp
done

A.4 The Consistency and Less Informative Relations

inductive consistent :: $ty \Rightarrow ty \Rightarrow bool$ (infix $\sim$ 51)
where
  CRefl[intro!]: $\tau \sim \tau$
  CFun[intro!]: $[ \sigma \sim \tau; \sigma' \sim \tau' ] \Rightarrow (\sigma \rightarrow \sigma') \sim (\tau \rightarrow \tau')$
  CUnR[intro!]: $\tau \sim ?$
  CUnL[intro!]: $? \sim \tau$

lemma consistent-reflexive: $\sigma \sim \sigma$
  apply (induct rule: ty.induct) apply auto done
lemma consistent-symmetric: \( \sigma \sim \tau \implies \tau \sim \sigma \)
apply (induct rule: consistent.induct) by auto

lemma consistent-not-trans:
\( \neg (\forall \tau_1 \tau_2 \tau_3. \tau_1 \sim \tau_2 \land \tau_2 \sim \tau_3 \implies \tau_1 \sim \tau_3) \)
proof
have A: IntT \sim ? by auto
have B: ? \sim BoolT by auto
have C: \( \neg (IntT \sim BoolT) \) by auto
from A B C show \(?thesis by auto
qed

inductive less-info :: ty \Rightarrow ty \Rightarrow bool (infixl \subseteq 51)
where
LEInt[intro!]: IntT \subseteq IntT |
LEBool[intro!]: BoolT \subseteq BoolT |
LEUVar[intro!]: UVarT \alpha \subseteq UVarT \alpha |
LEFun[intro!]: [ \sigma \subseteq \tau; \sigma' \subseteq \tau' ] \implies (\sigma \to \sigma') \subseteq (\tau \to \tau') |
LEBottom[intro!]: ? \subseteq \tau

lemma less-info-refl[intro!]: t \subseteq t
apply (induct t) by auto
lemma less-info-transitive-impl:
\( \forall \varrho \tau. \varrho \subseteq \sigma \land \sigma \subseteq \tau \implies \varrho \subseteq \tau \)
apply (induct \sigma) apply blast+ done

using less-info-transitive-impl by blast
lemma less-info-transitive: [ \varrho \subseteq \sigma; \sigma \subseteq \tau ] \implies \varrho \subseteq \tau
lemma less-info-implies-consistent: \sigma \subseteq \tau \implies \sigma \sim \tau
apply (induct rule: less-info.induct) by auto
lemma less-cons-implies-cons[rule-format]: \sigma \subseteq \tau \implies (\forall \tau'. \tau \sim \tau' \implies \sigma \sim \tau')
apply (induct rule: less-info.induct)
simp
apply simp
apply simp
apply clarify
apply (erule cons-fun-any)
simp
apply (erule-tac x=\tau in allE)
simp
apply (erule-tac x=\tau' in allE)
force
apply simp apply blast
simp
apply (erule-tac x=\tau'' in allE)
simp
apply (erule-tac x=\tau'b in allE)
force
apply force
done

lemma cons-less-less: t_1 \sim t_2 \implies (\exists \ t_3. t_1 \subseteq t_3 \land t_2 \subseteq t_3)
apply (induct rule: consistent.induct) apply blast+ done
lemmas less-less-cons [rule-format]: $t_1 \subseteq t_2 \implies (\forall t_3, t_3 \subseteq t_2 \implies t_1 \sim t_3)$

apply (induct rule: less-info.induct)

apply clarify apply (rule consistent-symmetric)

apply (rule less-info-implies-consistent) apply assumption

apply blast

apply blast

apply blast

apply blast

apply blast

apply blast

done

A.5 The Gradual Type System

inductive gtlc-wt :: env $\Rightarrow$ [expr,ty] $\Rightarrow$ bool ($\vdash \cdot \cdot \vdash \cdot \cdot \cdot \vdash [52,52,52] 51$)

where

WTVar [intro!]: $[\text{lookup } \Gamma x = \text{Some } \tau ] \Longrightarrow \Gamma \vdash \text{Var } x : \tau$

WTConst [intro!]: $\Gamma \vdash \text{Const } c : \text{TypeOf } c$

WTAbs [intro!]: $[x, \tau] \# \Gamma \vdash e : \sigma \Longrightarrow \Gamma \vdash (\lambda x : \tau. e) : \tau \rightarrow \sigma$

WTApp1 [intro!]: $[\Gamma \vdash g e : ?; \Gamma \vdash e' : \tau ] \Longrightarrow \Gamma \vdash (\text{App } e e') : ?$

WTApp2 [intro!]: $[\Gamma \vdash e : \tau \rightarrow g; \Gamma \vdash e' : \tau'; \tau' \sim \tau ]$

$\Longrightarrow \Gamma \vdash (\text{App } e e') : g$

A.6 Consistent-equal and Consistent-less

inductive consistent-equal :: subst $\Rightarrow$ [ty, ty] $\Rightarrow$ bool ($\vdash \cdot \cdot \cdot \vdash \cdot \cdot \cdot \cdot \vdash [50,50,50] 51$)

and consistent-less :: subst $\Rightarrow$ [ty, ty] $\Rightarrow$ bool ($\vdash \cdot \cdot \cdot \vdash \cdot \cdot \cdot \cdot \vdash [50,50,50] 51$)

where

CEInt [intro!]: $S \vdash \text{IntT} \simeq \text{IntT}$

CBeq [intro!]: $S \vdash \text{BoolT} \simeq \text{BoolT}$

CEDynL [intro!]: $S \vdash ? \simeq \tau$

CEDynR [intro!]: $S \vdash \tau \simeq ?$

CEFun [intro!]: $[S \vdash \sigma \simeq \tau; S \vdash \sigma' \simeq \tau'] \Longrightarrow S \vdash (\sigma \rightarrow \sigma') \simeq (\tau \rightarrow \tau')$

CEVarR [intro!]: $S \vdash \tau \subseteq \%S \alpha \Longrightarrow S \vdash \tau \simeq \text{UVarT } \alpha$

CEVarL [intro!]: $S \vdash \tau \subseteq \%S \alpha \Longrightarrow S \vdash \text{UVarT } \alpha \simeq \tau$

CLVar [intro!]: $\%S \alpha = \tau \Longrightarrow S \vdash \text{UVarT } \alpha \subseteq \tau$

CLIn [intro!]: $S \vdash \text{IntT } \subseteq \text{IntT}$

CLBool [intro!]: $S \vdash \text{BoolT } \subseteq \text{BoolT}$

CLDynL [intro!]: $S \vdash ? \subseteq \tau$

CLFun [intro!]: $S \vdash \sigma \subseteq \tau; S \vdash \sigma' \subseteq \tau' \Longrightarrow S \vdash (\sigma \rightarrow \sigma') \subseteq (\tau \rightarrow \tau')$

A.6.1 Properties of Consistent-equal/less

The following lemmas correspond to Proposition 1 of the paper.

lemma consless-refl: $S \vdash t \subseteq S t$ apply (induct t) by auto

lemma consless-trans-impl: $(S \vdash \tau 1 \simeq \tau 2 \longrightarrow \text{True})$

$\land (S \vdash \tau 2 \subseteq \tau 3 \longrightarrow (\forall \tau 1, \tau 1 \subseteq \tau 2 \longrightarrow S \vdash \tau 1 \subseteq \tau 3))$

apply (induct rule: consistent-equal-consistent-less.induct) by auto

lemma consless-trans: $[\tau 1 \subseteq \tau 2; S \vdash \tau 2 \subseteq \tau 3 ] \Longrightarrow S \vdash \tau 1 \subseteq \tau 3$

using consless-trans-impl by blast
lemma \textit{conseq-refl}: $\Gamma \vdash \tau \simeq \tau$
apply (induct \(\tau\)) \textbf{apply} blast+ \textbf{done}

lemma \textit{conseq-symm-impl}: $(\Gamma \vdash \tau \simeq \tau' \rightarrow \Gamma \vdash \tau' \simeq \tau) \land (\Gamma \vdash \tau \subseteq \tau' \rightarrow \text{True})$
apply (induct rule: consistent-equal-consistent-less.induct)
apply \textbf{auto}
done

lemma \textit{conseq-symm}: $\Gamma \vdash \tau \simeq \tau' \rightarrow \Gamma \vdash \tau' \simeq \tau$
\textbf{using} \textit{conseq-symm-impl} \textbf{by} blast

lemma \textit{conseq-less-no-dyn-equal-impl}:
$(\Gamma \vdash \tau \simeq \tau_1 \rightarrow \text{no-dyn } \tau_1 \land \text{no-dyn } \tau_2 \rightarrow \presupp S \tau_1 = \presupp S \tau_2)$
\land $(\Gamma \vdash \tau \subseteq \tau' \rightarrow \text{no-dyn } \tau \rightarrow \presupp S \tau = \tau')$
apply (induct rule: consistent-equal-consistent-less.induct)
apply \textbf{simp+}
done

lemma \textit{conseq-less-no-dyn-equal}:
\[ [\Gamma \vdash \tau \simeq \tau_1 ; \text{no-dyn } \tau; \text{no-dyn } \tau'] \rightarrow \presupp S \tau = \presupp S \tau' \]
\textbf{using} \textit{conseq-less-no-dyn-equal-impl} \textbf{by} blast

lemma \textit{less-no-dyn-equal}:
\[ [\Gamma \vdash \tau \subseteq \tau_1 ; \text{no-dyn } \tau ] \rightarrow \presupp S \tau = \tau' \]
\textbf{using} \textit{conseq-less-no-dyn-equal-impl} \textbf{by} blast

lemma \textit{less-conseq-less-impl}:
$(\Gamma \vdash \tau \simeq \tau_1 \rightarrow \text{True})$
\land $(\Gamma \vdash \tau \subseteq \tau' \rightarrow \text{no-dyn } \tau \rightarrow$
$(\forall \tau', \text{no-dyn } \tau' \land \Gamma \vdash \tau \simeq \tau' \rightarrow \Gamma \vdash \tau' \subseteq \tau''))$
apply (induct rule: consistent-equal-consistent-less.induct)
apply simp apply simp apply simp apply simp apply simp apply simp apply simp apply simp apply (rule impl1) apply simp apply (case_tac no-dyn \(\sigma\)) \textbf{apply} simp
prefer 2 \textbf{apply} simp
apply clarify
apply (erule \textit{conseq-fun-any})
apply simp apply simp
apply (case_tac no-dyn \(\tau''\)) \textbf{apply} simp
prefer 2 \textbf{apply} simp
apply (rule \textit{CLFun})
apply force
apply force
apply simp
apply (rule \textit{CLVar})
apply (erule \textit{conslless-fun-any})
apply simp
apply simp
apply (rule conjI)

proof –
\textbf{fix} \(S \sigma \sigma' \tau \tau' \tau'a \alpha \tau'' \tau'b\)
\textbf{assume} \(st: \Gamma \vdash \tau \subseteq \tau \text{ and } ns: \text{no-dyn } \sigma \text{ and } \text{stt: } \Gamma \vdash \sigma \subseteq \tau''\)
\textbf{from} \(st \text{ ns} \text{ have} \text{ stt: } \presupp S \sigma = \tau \text{ by (rule less-no-dyn-equal)}\)
\textbf{from} \(stt \text{ ns} \text{ have} \presupp S \sigma = \tau'' \text{ by (rule less-no-dyn-equal)}\)
with sst show $\tau'' = \tau$ by simp

next
  fix $S \sigma \sigma' \tau \tau' a \alpha \tau'' \tau'b$
  assume st: $S \vdash \sigma' \subseteq \tau' \text{ and } ns: \text{no-dyn } \sigma'$ and stt: $S \vdash \sigma' \subseteq \tau'b$
  from st ns have sst: $S \sigma' = \tau'$ by (rule less-no-dyn-equal)
  from stt ns have sst: $S \sigma' = \tau'b$ by (rule less-no-dyn-equal)
  with sst show $\tau'b = \tau'$ by simp
qed

lemma less-conseq-less: $[ [ S \vdash \tau \subseteq \tau'' \text{; no-dyn } \tau \text{; no-dyn } \tau' \text{; } S \vdash \tau \simeq \tau' ] ]$
  $\Rightarrow S \vdash \tau' \subseteq \tau''$
using less-conseq-less-impl by blast

lemma less-less-conseq-impl:
  $(S \vdash \tau \simeq \tau' \longrightarrow True) \land$
  $(S \vdash \tau \subseteq q \longrightarrow (\forall \tau'. S \vdash \tau' \subseteq q \longrightarrow S \vdash \tau \simeq \tau'))$
apply (induct rule: consistent-equal-consistent-less.induct)
apply simp+ apply blast apply force apply force apply force apply force
apply clarify apply (rule consless-any-fun) apply auto done

lemma less-less-conseq:
  $[[ S \vdash \tau \subseteq g; S \vdash \tau' \subseteq g ]] \Rightarrow S \vdash \tau \simeq \tau'$
using less-less-conseq-impl by blast

lemma subst-typeof: $S (\text{TypeOf } c) = \text{TypeOf } c$
apply (case-tac c) apply auto done

lemma subst-const: $S (\text{Const } c) = \text{Const } c$
apply (case-tac c) apply auto done

lemma subst-extend-env: $S ((x, \tau)\#\Gamma) = (x, S \tau)\#(S \Gamma)$
by (simp add: app-subst-pair)

lemma cons-any-fun2:
  $\tau \sim t1 \rightarrow t2 \Longrightarrow (\tau = ?) \lor (\exists s1 s2. \tau = s1 \rightarrow s2 \land s1 \sim t1 \land s2 \sim t2)$
using cons-any-fun by blast

lemma ce-less-implies-cons-less:
  $(S \vdash \tau \simeq \tau' \longrightarrow S S \tau \sim S \tau') \land (S \vdash \tau \subseteq \tau' \longrightarrow S S \tau \subseteq \tau')$
apply (induct rule: consistent-equal-consistent-less.induct)
apply force apply force apply force apply force
apply simp apply (rule CFun) apply simp apply simp apply simp
apply simp using less-info-implies-consistent apply blast
apply simp apply (frule less-info-implies-consistent) apply simp
apply (frule consistent-symmetric) apply simp
apply force+
done

lemma cons-eq-implies-cons:
\[ S \vdash \tau \equiv \tau' \implies \$S \tau \sim \$S \tau' \]
using \texttt{ce-less-implies-cons-less by blast}

\textbf{lemma cons-less-implies-less:}
\[ S \vdash \tau \sqsubseteq \tau' \implies \$S \tau \sqsubseteq \tau' \]
using \texttt{ce-less-implies-cons-less by blast}

\textbf{lemma conseq-any-fun-var:}
\[ S \vdash \tau \equiv \tau' \implies UVarT \beta \implies \\
\tau \equiv ? \lor (\exists t_1 t_2. \$S \tau = t_1 \rightarrow t_2 \land t_1 \sim \$S \tau' \land t_2 \sqsubseteq \%S \beta) \\
\text{apply \ (case-tac } \tau) \\
\text{defer} \\
\text{apply force} \\
\text{apply force} \\
\text{apply simp} \\
\text{apply simp} \\
\text{apply (erule conseq-fun-fun) apply (rule conjI)} \\
\text{apply (rule cons-eq-implies-cons) apply simp} \\
\text{apply (erule conseq-any-var) apply simp} \\
\text{apply (rule cons-less-implies-less) apply simp} \\
\text{apply simp} \\
\text{apply (erule consless-var-any) apply force}
\]
\textbf{proof --}
\begin{itemize}
\item fix \( \alpha \) assume \( t : S \vdash \tau \equiv \tau' \rightarrow UVarT \beta \) and \( t : \tau = UVarT \alpha \)
\item from \( t : \text{apply apply (erule conseq-var-fun) by blast} \)
\item from \( t : \text{obtain } t_1 \ t_2 \text{ where } t_1 : S \vdash \tau' \sqsubseteq t_1 \text{ and } t_2 : S \vdash UVarT \beta \sqsubseteq t_2 \)
\item and \( \text{sa: } \%S \alpha = t_1 \rightarrow t_2 \text{ using conseq-fun-var-any by blast} \)
\item from \( t : \text{apply simp apply force} \)
\item hence \( t : \text{using less-info-implies-consistent consistent-symmetric by blast} \)
\item hence \( t : \text{by force} \)
\item from \( t : \text{show } \tau = ? \lor (\exists t_1 t_2. \$S \tau = t_1 \rightarrow t_2 \land t_1 \sim \$S \tau' \land t_2 \sqsubseteq \%S \beta) \text{ by simp} \)
\end{itemize}
\textbf{qed}

\textbf{lemma conseq-any-fun-rule:}
\[ \[ S \vdash \tau \equiv \tau' \rightarrow UVarT \beta; \]
\[ \tau = ? \implies P; \]
\[ \land \ t_1 t_2. \ [ \$S \tau = t_1 \rightarrow t_2; t_1 \sim \$S \tau' \land t_2 \sqsubseteq \%S \beta ] \implies P \]
\[ \implies P \]
\text{apply (erule conseq-any-var) apply (erule disjE)}
\text{apply simp}
\text{apply (erule exE)+ apply simp apply clarify}
\text{apply (case-tac } \$S \tau) \text{ apply force apply force apply force apply force apply force}
\text{apply simp apply clarify apply simp}
\textbf{proof --}
\begin{itemize}
\item fix \( t \ t_1 \ t_2 \)
\item assume \( A : \land t_1 t_2 a. \ [ t_1 = t_1 a \land t_2 t_2 a; t_1 a \sim \$ S \tau' \land t_2 a \sqsubseteq \%S \beta ] \implies P \)
\item and \( B : t_1 \sim \$ S \tau' \text{ and } C : t_2 \sqsubseteq \%S \beta \)
\item from \( A[t_1 t_2] \text{ B C show P apply blast done} \)
\end{itemize}
\textbf{qed}

\textbf{lemma prop1-item-6-and-7-fwd:}
\[ (S \vdash t_1 \equiv t_2 \implies FTV t_1 = \{ \} \land FTV t_2 = \{ \} \implies t_1 \sim t_2) \]

37
\begin{itemize}
\item \((S ⊢ t_1 ⊆ t_2 \longrightarrow FTV \ t_1 = \{\} \longrightarrow t_1 ⊆ t_2)\)
\item \texttt{apply (induct rule: consistent-equal-consistent-less.induct)}
\item \texttt{apply blast apply blast apply blast apply blast}
\item \texttt{apply clarify apply simp apply (rule CFun) apply simp apply simp}
\item \texttt{apply simp apply simp apply blast apply blast apply blast apply blast}
\item \texttt{apply clarify apply (rule LEFun) apply simp apply simp}
\item \texttt{done}
\end{itemize}

\textbf{lemma prop1-item-6-back:}
\(t_1 \sim t_2 \implies FTV \ t_1 = \{\} \land FTV \ t_2 = \{\} \implies (\forall S. S \vdash t_1 \sim t_2)\)
\texttt{apply (induct rule: consistent.induct)}
\texttt{apply clarify apply (rule conseq-refl)}
\texttt{apply clarify apply (rule CFun) apply simp apply simp}
\texttt{apply blast apply blast done}

\textbf{lemma ftv-empty-subst-id[rule-format]:}
\(\forall S. FTV \ \tau = \{\} \longrightarrow \$S \ \tau = (\tau::ty)\)
\texttt{apply (induct \(\tau\) \ by \ auto)

\textbf{lemma prop1-item-7-back:}
\(t_1 \subseteq t_2 \implies FTV \ t_1 = \{\} \rightarrow (\forall S. S \vdash t_1 \subseteq t_2)\)
\texttt{apply (induct rule: less-info.induct)}
\texttt{apply blast}
\texttt{defer}
\texttt{apply clarify apply (rule CLFun) apply simp apply simp}
\texttt{apply blast}
\texttt{apply auto}
\texttt{done}

\textbf{lemma widen-conseq-consless:}
\((S \vdash \alpha \sim \tau_2 \longrightarrow (\forall \alpha. \alpha \in FTV \ \tau_1 \cup FTV \ \tau_2 \longrightarrow \%S' \ \alpha = \%S \ \alpha) \rightarrow S' \vdash \tau_1 \sim \tau_2)\)
\texttt{apply (induct rule: consistent-equal-consistent-less.induct)}
\texttt{apply force+ done}

\textbf{lemma widen-conseq:}
\[
\begin{array}{l}
[S \vdash \tau_1 \sim \tau_2; (\forall \alpha. \alpha \in FTV \ \tau_1 \cup FTV \ \tau_2 \longrightarrow \%S' \ \alpha = \%S \ \alpha)] \\
\implies S' \vdash \tau_1 \sim \tau_2
\end{array}
\]
\texttt{using widen-conseq-consless by blast}

\textbf{lemma widen-consless:}
\[
\begin{array}{l}
[S \vdash \tau_1 \subseteq \tau_2; (\forall \alpha. \alpha \in FTV \ \tau_1 \longrightarrow \%S' \ \alpha = \%S \ \alpha)] \\
\implies S' \vdash \tau_1 \subseteq \tau_2
\end{array}
\]
\texttt{using widen-conseq-consless by blast}

\section{A.7 The Gradual Type System with Type Variables}
\texttt{inductive igtc-ut :: subst \circ \ env \circ nat \circ nat \Rightarrow [expr,ty] \Rightarrow bool (-;:-;:: \vdash g - :: [52,52,52,52,52,52,52] 51) where}
\texttt{GVar[intro]: \{ lookup \(\Gamma\) \(x\) = Some \(\tau\) \} \Rightarrow S;\Gamma;n;g \vdash \ Var x : \tau \ |
\texttt{GConst[intro]: S;\Gamma;n;g \vdash \ Const \ c : \ TypeOf \ c \ |
\texttt{GAbs[intro]: S;\(\times,\tau_1\)#\Gamma;m;g \vdash \ e : \tau_2 \} \Rightarrow S;\Gamma;m;g \vdash (\lambda x:\tau_1. \ e) : \tau_1 \rightarrow \tau_2 \ |
GApp[intro]: \[ S;\Gamma;\alpha \vdash e : \tau_1; \Gamma;\alpha ;n1 \vdash e' : \tau_2; \\
S \vdash \tau_1 \simeq (\tau_2 \rightarrow \text{UVarT } n2) \]
\[ \Rightarrow S;\Gamma;\alpha ;\text{Suc } n2 \vdash (\text{App } e e') : \text{UVarT } n2 \]

**lemma** ftv-env-ftv-ty[rule-format]:
\[ \forall \alpha. \text{lookup } \Gamma \ x = \text{Some } \tau \rightarrow \text{FTV } \tau \subseteq \text{FTV } \Gamma \]

**apply** (induct \( \Gamma \)) by auto

**lemma** igtlc-fresh-grows:
\[ S;\Gamma;m:n \vdash e : \tau \Rightarrow m \leq n \]

**apply** (induct rule: igtlc-ut.induct)

**apply** simp+ done

**lemma** igtlc-ftv-result:
\[ S;\Gamma;m:n \vdash e : \tau \Rightarrow (\forall \alpha. \alpha \in \text{FTV } \tau \rightarrow \alpha \in \text{FTV } \Gamma \cup \text{FTV } e \cup (m \leq \alpha \land \alpha < n)) \]
(is \[ S;\Gamma;m:n \vdash e : \tau \Rightarrow \exists P.S \Gamma m n e \tau \]

**apply** (induct rule: igtlc-ut.induct)

**apply** clarify apply simp using ftv-env-ftv-ty apply blast

**apply** simp apply clarify apply (case-tac e) apply simp apply simp apply simp apply simp

**proof** –

**fix** \( S \Gamma \tau_1 \tau_2 m n x \)

**assume** \( S;x;\tau_1;\#\Gamma;m:n \vdash e : \tau_2 \)

and \( IH: \forall \alpha. \alpha \in \text{FTV } \tau_2 \rightarrow \alpha \in \text{FTV } ((x;\tau_1;\#\Gamma) \cup \text{FTV } e \cup m \leq \alpha \land \alpha < n) \)

**show** \[ \exists P.S \Gamma m n (\lambda x;\tau_1; e) (\tau_1 \rightarrow \tau_2) \]

**apply** (rule allI) apply (rule.impl)

**proof** –

**fix** \( \alpha \) assume \( af12: \alpha \in \text{FTV } (\tau_1 \rightarrow \tau_2) \)

from \( af12 \) have \( \alpha \in \text{FTV } \tau_1 \lor \alpha \in \text{FTV } \tau_2 \) by simp

**moreover** { assume \( af1: \alpha \in \text{FTV } \tau_1 \)

from \( af1 \) have \( \alpha \in \text{FTV } (\lambda x;\tau_1; e) \) by simp

**hence** \( \alpha \in \text{FTV } \Gamma \cup \text{FTV } (\lambda x;\tau_1; e) \lor m \leq \alpha \land \alpha < n \) by simp

} **moreover** { assume \( af2: \alpha \in \text{FTV } \tau_2 \)

from \( af2 \) have \( \alpha \in \text{FTV } ((x;\tau_1;\#\Gamma) \cup \text{FTV } e \lor m \leq \alpha \land \alpha < n) \) by simp

**moreover** { assume \( \alpha \in \text{FTV } ((x;\tau_1;\#\Gamma) \)

**hence** \( \alpha \in \text{FTV } \Gamma \lor \alpha \in \text{FTV } \tau_1 \) apply (simp add: FTV-pair) by blast

**hence** \( \alpha \in \text{FTV } \Gamma \cup \text{FTV } (\lambda x;\tau_1; e) \lor m \leq \alpha \land \alpha < n \) by force

} **moreover** { assume \( \alpha \in \text{FTV } e \)

**hence** \( \alpha \in \text{FTV } (\lambda x;\tau_1; e) \) by simp

**hence** \( \alpha \in \text{FTV } \Gamma \cup \text{FTV } (\lambda x;\tau_1; e) \lor m \leq \alpha \land \alpha < n \) by simp

} **moreover** { assume \( m \leq \alpha \land \alpha < n \)

**hence** \( \alpha \in \text{FTV } \Gamma \cup \text{FTV } (\lambda x;\tau_1; e) \lor m \leq \alpha \land \alpha < n \) by simp

} **ultimately** have \( \alpha \in \text{FTV } \Gamma \cup \text{FTV } (\lambda x;\tau_1; e) \lor m \leq \alpha \land \alpha < n \) by blast

} **ultimately** show \( \alpha \in \text{FTV } \Gamma \cup \text{FTV } (\lambda x;\tau_1; e) \lor m \leq \alpha \land \alpha < n \) by blast

**qed**

**next**

**fix** \( S \Gamma \tau_1 \tau_2 e e' n0 n1 n2 \)

**assume** \( \text{wte: } S;\Gamma;n0:n1 \vdash e : \tau_1 \)

and \( IH1: \forall \alpha. \alpha \in \text{FTV } \tau_1 \rightarrow \alpha \in \text{FTV } \Gamma \cup \text{FTV } e \lor n0 \leq \alpha \land \alpha < n1 \)

and \( \text{wtep: } S;\Gamma;n1:n2 \vdash e' : \tau_2 \)

and \( IH2: \forall \alpha. \alpha \in \text{FTV } \tau_2 \rightarrow \alpha \in \text{FTV } \Gamma \cup \text{FTV } e' \lor n1 \leq \alpha \land \alpha < n2 \)

and \( s12b: S \vdash \tau_1 \simeq \tau_2 \rightarrow \text{UVarT } n2 \)

**show** \( \forall \alpha. \alpha \in \text{FTV } (\text{UVarT } n2) \rightarrow \alpha \in \text{FTV } \Gamma \cup \text{FTV } (\text{App } e e') \lor n0 \leq \alpha \land \alpha < \text{Suc } n2 \)

**apply** (rule allI) apply (rule.impl)

**proof** –

**fix** \( \alpha \) assume \( \alpha \in \text{FTV } (\text{UVarT } n2) \) hence \( \text{an2: } \alpha = n2 \) by simp
from an2 have asn2: α < Suc n2 by simp
from wte have n0n1: n0 ≤ n1 by (rule igtlc-fresh-grows)
from wtep have n1n2: n1 ≤ n2 by (rule igtlc-fresh-grows)
from n0n1 n1n2 an2 have n0a: n0 ≤ α by simp
from n0a an2
show α ∈ FTV Γ ∪ FTV (App e e') ∨ n0 ≤ α ∧ α < Suc n2 by simp
qed

lemma widen-subst-impl:
S:Γ;m;n ⊢ g e : τ  
(∀ α. α ∈ FTV Γ ∪ FTV e ∨ (m ≤ α ∧ α < n) → %S' α = %S α)  
→ S':Γ;m;n ⊢ g e : τ
(is S:Γ;m;n ⊢ g e : τ → ?P S Γ m n e τ)
apply (induct rule: igtlc-ut.induct)
apply force
apply force

proof

fix S Γ τ1 τ2 e m n x
assume S:(x,τ1)#Γ;m;n ⊢ g e : τ2  
and IH: (∀ α. α ∈ FTV ((x,τ1)#Γ) ∪ FTV e ∨ m ≤ α ∧ α < n → %S' α = %S α)  
→ S':(x,τ1)#Γ;m;n ⊢ g e : τ2
show (∀ α. α ∈ FTV Γ ∪ FTV (λx:τ1. e) ∨ m ≤ α ∧ α < n → %S' α = %S α)  
→ S':Γ;m;n ⊢ g e : τ1 → τ2

proof clarify
assume b7: ∀ α. α ∈ FTV Γ ∪ FTV (λx:τ1. e) ∨ m ≤ α ∧ α < n → %S' α = %S α
from b7 have (∀ α. α ∈ FTV ((x,τ1)#Γ) ∪ FTV e ∨ m ≤ α ∧ α < n → %S' α = %S α)  
apply clarify apply (erule disjE)
apply simp apply (erule disjE)
apply (erule-tac x=α in allE) apply (simp add: FTV-pair)
apply blast
apply blast

done

with IH show S':(x, τ1)#Γ;m;n ⊢ g e : τ2 by simp
qed

next

fix S Γ τ1 τ2 e' n0 n1 n2
assume wte: S:Γ;n0:n1 ⊢ g e : τ1  
and wtep: S:Γ;n1:n2 ⊢ g e' : τ2  
and IH1: ?P S Γ n0 n1 e τ1  
and st12b: S ⊢ τ1 ≃ τ2  → UVarT n2
show ?P S Γ n0 (Suc n2) (App e e') (UVarT n2)

proof clarify
assume fa: ∀ α. α ∈ FTV Γ ∪ FTV (App e e') ∨ n0 ≤ α ∧ α < Suc n2 → %S' α = %S α
from wte have n0n1: n0 ≤ n1 by (rule igtlc-fresh-grows)
from wtep have n1n2: n1 ≤ n2 by (rule igtlc-fresh-grows)
from fa n1n2
have fe: (∀ α. α ∈ FTV Γ ∪ FTV e ∨ n0 ≤ α ∧ α < n1 → %S' α = %S α) by simp
from fe IH1 have wtep': S:Γ;n0:n1 ⊢ g e : τ1 by simp
from fa n0n1
have fep: (∀ α. α ∈ FTV Γ ∪ FTV e' ∨ n1 ≤ α ∧ α < n2 → %S' α = %S α) by simp
from fep IH2 have wtep2: S:Γ;n1:n2 ⊢ g e' : τ2 by simp
from wte2 fe have af1: (∀ α. α ∈ FTV τ1 → %S' α = %S α)
using igtlc-ftv-result apply blast done
from wtep2 fep have aft2: (∀ α. α ∈ FTV τ₂ → %S' α = %S α)
using igtlc-ftv-result apply blast done
from wte have n0n1: n0 ≤ n1 by (rule igtlc-fresh-grows)
from wtep have n1n2: n1 ≤ n₂ by (rule igtlc-fresh-grows)
from fa n0n1 n1n2 have (∀ α. α ∈ FTV (UVarT n₂) → %S' α = %S α) by auto
with aft1 aft2
have aft2b: (∀ α. α ∈ FTV τ₁ ∪ FTV τ₂ → %S' α = %S α) by simp
from st2b aft12b have S’ ⊓ τ₁ ∼ τ₂ → UVarT n₂ by (rule widen-conseq)
with wte2 wtep2 show S’;Γ;n0;Suc n2 ⊢ App e e’ : UVarT n₂ by blast
qed

— Theorem 2

theorem igtlc-implies-glč:
S;Γ;m;n ⊢ g e : τ; (∀ α. α ∈ FTV Γ ∪ FTV e ∨ (m ≤ α ∧ α < n) → %S’ α = %S α)
⇒ S’;Γ;m;n ⊢ g e : τ
using widen-subst-impl by blast

lemma widen-subst:
[ S;Γ;m;n ⊢ g e : τ; (∀ α. α ∈ FTV Γ ∪ FTV e ∨ (m ≤ α ∧ α < n) → %S’ α = %S α) ]
⇒ S’;Γ;m;n ⊢ g e : τ
using widen-subst-impl by blast

next
fix Γ:env and τ and x and S n assume gx: lookup Γ x = Some τ
show ?P S Γ (Var x) τ
proof clarify
assume fg: FTV Γ = {} from gx fg have FTV τ = {} using ftv-env-ftv-ty by blast
hence ∀ a. a ∈ FTV τ → %S a = UVarT a by simp
hence %S τ = τ using ftv-dom-id by blast
hence τ ⊑ %S τ apply simp by (rule less-info-refl)
with gx show ∃ τ’. Γ ⊢ g Var x : τ’ ∧ τ’ ⊑ %S τ by blast
qed

next
fix S Γ c show ?P S Γ (Const c) (TypeOf c) by auto

next
fix S:subt and x τ₁ and Γ::env and m n e τ₂
assume IH: ?P S ((x,τ₁)#Γ) e τ₂
show ?P S Γ (λx:τ₁. e) (τ₁ → τ₂)
proof clarify
assume fg: FTV Γ = {} and fl: FTV (λx:τ₁. e) = {}
from fl have ft: FTV τ₁ = {} by simp
with fg have fg2: FTV ((x,τ₁)#Γ) = {} by (simp add: FTV-fun)
from fl have fe: FTV e = {} by simp
from fg2 fe IH obtain τ’ where wte: (x,τ₁)#Γ ⊢ g e : τ’
and tps: τ’ ⊑ %S τ₂ by blast
from ft have ∀ a. a ∈ FTV τ₁ → %S a = UVarT a by simp
hence %S τ₁ = τ₁ using ftv-dom-id by blast
with tps have stt: τ₁ → τ’ ⊑ %S (τ₁ → τ₂) apply simp apply (rule LEFun) apply (rule less-info-refl) apply simp done
from wte have Γ ⊢ g (λx:τ₁. e) : τ₁ → τ’ by blast
with stt show ∃ τ’. Γ ⊢ g (λx:τ₁. e) : τ’ ∧ τ’ ⊑ %S (τ₁ → τ₂) apply (rule tac x=τ₁ → τ’ in exI)
apply simp done
qed
next
fix $S \Gamma n0 n1 e \tau_1 n2 e' \tau_2$
assume $IH1$: $?P S \Gamma e \tau_1$
and $IH2$: $?P S \Gamma e' \tau_2$
and $st12b$: $S \vdash \tau_1 \simeq \tau_2 \rightarrow UVar T n2$
show $?P S \Gamma (App e e') (UVar T n2)$
proof clarify
assumef $fg$: $FTV \Gamma = \{\}$ and $fa$: $FTV (App e e') = \{\}$
from $fa$ have $fc$: $FTV e = \{\}$ by simp
with $fg$ $IH1$ obtain $t1$ where wtep: $\Gamma \vdash_g e : t1$ and $t11 \sqsubseteq S \tau_1$ by blast
from $fa$ have $fcp$: $FTV e' = \{\}$ by simp
with $fg$ $IH2$ obtain $t2$ where wtep: $\Gamma \vdash_g e' : t2$
and $st2$: $t2 \sqsubseteq S \tau_2$ by blast
from $st12b$ show $\exists \tau' . \Gamma \vdash_g App e e' : \tau' \land \tau' \sqsubseteq S (UVar T n2)$
proof (rule conseq-any-fun-var-rule)
assume $t1d$: $\tau_1 = ?$
with $t11$ have $T1d$: $t1 = ?$ by auto
from wtep $T1d$ have wtep2: $\Gamma \vdash_g e : ?$ by simp
with wtep have $A$: $\Gamma \vdash_g App e e' : ?$ by blast
have $B$: $? \sqsubseteq S (UVar T n2)$ by blast
from $A B$ show $\text{thesis}$ by blast
next
fix $t11 t12$ assume $st1$: $S \tau_1 = t11 \rightarrow t12$ and $t11st2$: $t11 \sim S \tau_2$
and $st2$: $t12 \sqsubseteq \%S n2$
from $t11 st1$ have $t1-le-t12$: $t1 \sqsubseteq t11 \rightarrow t12$ by simp
from $t11st2$ have $st21$: $S \tau_2 \sim t11$ by (rule consistent-symmetric)
from $t1-le-t12$ show $\text{thesis}$
proof (rule le-any-fun-
fix $\sigma \sigma'$ assume $st11$: $\sigma \sqsubseteq t11$ and $st12$: $\sigma' \sqsubseteq t12$
and $T1$: $t1 = \sigma \rightarrow \sigma'$
with wtep have wtep2: $\Gamma \vdash_g e : \sigma \rightarrow \sigma'$ by simp
from $st12 st211$ have $t211$: $t2 \sim t11$ by (rule less-cons-implies-cons)
hence $t11t2$: $t11 \sim t2$ by (rule consistent-symmetric)
from $st11 t11t2$ have $\sigma \sim t2$ by (rule less-cons-implies-cons)
hence $t2$: $t2 \sim \sigma$ by (rule consistent-symmetric)
from wtep $t2$ have $A$: $\Gamma \vdash_g App e e' : \sigma' \vdash \text{by blast}$
from $st12 t2sb$ have $\sigma' \sqsubseteq \%S n2$ by (rule less-info-transitive)
hence $B$: $\sigma' \sqsubseteq S (UVar T n2)$ by simp
from $A B$ show $\exists \tau' . \Gamma \vdash_g App e e' : \tau' \land \tau' \sqsubseteq S (UVar T n2)$ by blast
next
assume $T1d$: $t1 = ?$
from wtep $T1d$ have wtep2: $\Gamma \vdash_g e : ?$ by simp
with wtep have $A$: $\Gamma \vdash_g App e e' : ?$ by blast
have $B$: $? \sqsubseteq S (UVar T n2)$ by blast
from $A B$ show $\text{thesis}$ by blast
qed
qed
qed

lemma lookup-subst-subst:
lookup $\Gamma x = \text{Some } \tau \Rightarrow$ lookup ($S \Gamma x = \text{Some } (S \tau)$
apply (induct $\Gamma$)
apply simp
apply (case-tac a) apply (case-tac aa = x)
  apply (simp add: app-subst-pair)
  apply (simp add: app-subst-pair)
done

— Part 1 of Theorem 3 of the paper

**Proof** of igtlc-wt-implies-gtlc:

\[ S; \Gamma; n \vdash e : \tau \implies (\exists \tau'. S \Gamma \vdash \exists S e : \tau' \land \tau' \subseteq S \tau) \]

**Proof (induct rule: igtlc-wt.induct)**

1. **Fix** \( \Gamma; \text{enve} \) and \( \tau \times S \times n \) **assume** \( \text{lookup} \ \Gamma \ x = \text{Some} \ \tau \)
2. **Thus** \( \exists \tau'. S \Gamma \vdash S \ (\text{Var} \ x) : \tau' \land \tau' \subseteq S \tau \)
   - apply **simp apply** (rule-tac x = $S \tau$ in exI) **apply** (rule conjI)
3. **Apply** (rule WTVar) **apply** (simp add: lookup-subst-subst) **apply** blast **done**

**Next**

fix \( S \Gamma \ n \ e \) **show** \( \exists \tau'. S \Gamma \vdash \exists S \ (\text{Const} \ c) : \tau' \land \tau' \subseteq S \ (\text{TypeOf} \ c) \)
   - apply **simp apply** blast **done**

**Next**

fix \( S \times \tau_1 \ \Gamma \ m \ n \ e \ \tau_2 \)
   - **Assume** \( \text{IH}1: \exists \tau'. S \ ((x, \tau_1) \# \Gamma) \vdash \exists S e : \tau' \land \tau' \subseteq S \tau_1 \)
   - **And** \( \text{tst}: \exists \tau'. S \ (x, \tau_1) \# \Gamma \vdash \exists S e : \tau' \) **by** blast
   - from \( \text{tst} \) **have** \( \exists \tau'. \ S \ (x, \tau_1) \# \Gamma \vdash \exists S e : \tau' \) **by** (simp only: subst-extend-enve)
8. **Hence** \( \text{wte}: \exists \tau'. S \ (x, \tau_1) \# \Gamma \vdash \exists S e : \tau' \land \tau' \subseteq S \tau_2 \)
   - **And** \( \text{tst1}: \exists \tau'. S \ (x, \tau_1) \# \Gamma \vdash \exists S e : \tau' \land \tau' \subseteq S \tau_2 \)

from \( \text{IH1} \) **obtain** \( \tau'_1 \) **where** \( \text{wte}: \exists \tau'. S \ (x, \tau_1) \# \Gamma \vdash \exists S e : \tau' \land \tau' \subseteq S \tau_1 \)
   - **And** \( \text{tst1}: \exists \tau': S \ (x, \tau_1) \# \Gamma \vdash \exists S e : \tau' \land \tau' \subseteq S \tau_2 \)

**From** \( \text{tst2} \) **show** \( \exists \tau'. S \Gamma \vdash \exists S e : \tau' \land \tau' \subseteq S \ (\text{UVarT n} \ 2) \)
   - **Proof (rule conseq-ang-fun-var-rule)**
   - **Assume** \( \text{tst1}: \tau'_1 = ? \)
8. **From** \( \text{tst1} \) **have** \( \text{tstp1}: \tau'_1 = ? \) **by** auto
   - **With** \( \text{wte} \) **have** \( \text{wte}: \exists \tau'. S \ (x, \tau_1) \# \Gamma \vdash \exists S e : ? \) **by** simp
8. **From** \( \text{wte} \) **wtep** **have** \( \exists \tau'. S \ (x, \tau_1) \# \Gamma \vdash \exists S e : ? \) **by** (rule WTApp1)
   - **Thus** \( \exists \tau'. S \ (x, \tau_1) \# \Gamma \vdash \exists S e : ? \) **by** simp

**Next**

fix \( t1 \ t2 \)
   - **Assume** \( \text{st1}: S \tau_1 = t1 \to t2 \) **and** \( \text{st1s}: t1 \sim S \tau_2 \) **and** \( \text{t2b}: t2 \subseteq %S n \ 2 \)
   - **From** \( \text{tst1} \) **have** \( \text{tstp12}: t1' \subseteq t1 \to t2 \) **by** simp
   - **Hence** \( t1' = ? \lor (\exists \ t11 \ t12. \ t1' = t11 \to t12) \) **using le-ang-fun** **by** blast
   - **Moreover** \{ **Assume** \( t1p: t1' = ? \)
8. **With** \( \text{wte} \) **have** \( \text{wte}: S \ (x, \tau_1) \# \Gamma \vdash \exists S e : ? \) **by** simp
8. **From** \( \text{wte} \) **wtep** **have** \( \exists \tau'. S \ (x, \tau_1) \# \Gamma \vdash \exists S e : ? \) **by** (rule WTApp1)
   - **Hence** \( \exists \tau'. S \ (x, \tau_1) \# \Gamma \vdash \exists S e : ? \) **by** simp
8. **Apply** simp **by** blast
   - \} **Moreover** \{ **Assume** \( X: \exists t11 \ t12. \ t1' = t11 \to t12 \)
8. **From** \( X \) **obtain** \( t11 \ t12 \) **where** \( T1: t1' = t11 \to t12 \) **by** blast
8. **From** \( T1 \) **tstp12** **have** \( t111: t11 \subseteq t1 \) **by** blast

43
from T1 t1p12 have t12t2: t12 ⊆ t2 by blast
from wte T1 have wte2: $ S \Gamma \vdash_g S e : t11 \Rightarrow t12 \text{ by simp}
from t11t1 t1s have t11s1: t11 $ \Rightarrow $ \tau_2 by (rule less-cons-implies-cons)
hence st12t11: $ S \tau_2 \sim t11 \text{ by (rule consistent-symmetric)}
from tpst2 st2111 have t2111: t2' \sim t11 by (rule less-cons-implies-cons)
from wte2 wtep t2111 have wta: $ S \Gamma \vdash_g (\$S e) \sim \tau_2$ by (rule WTApp2)
from t12t2 t2b have t12b: t12 ⊆ %S n2 by (rule less-info-transitive)
from wta t12b have \exists \tau'. $ S \Gamma \vdash_g S (\text{App e e}'): \tau' \land \tau' \subseteq S (UVarT n2)
apply simp by blast
} ultimately show \exists \tau'. $ S \Gamma \vdash_g S (\text{App e e}'): \tau' \land \tau' \subseteq S (UVarT n2)
by blast
qed

-- This is Theorem 4 of the paper

lemma no-dyn-lookup:
\[ x \in \tau. [ [ \text{lookup} \quad \Gamma \quad x = \text{Some} \quad \tau; \quad \text{no-dyn} \quad \Gamma ] ] \Rightarrow \text{no-dyn} \quad \tau \]
apply (induct \Gamma)
apply simp
apply simp
apply simp apply (case-tac a) apply simp
apply (case-tac no-dyn b) apply simp
apply (case-tac aa = x) apply simp
apply simp apply simp
done

theorem igtlc-wt-no-dyn-implies-istlc:
\[ S; \Gamma: m:n \vdash_g e : \tau \Rightarrow \text{no-dyn} \quad \Gamma \quad \land \quad \text{no-dyn} \quad e \Rightarrow S; \Gamma \vdash e : \tau \land \text{no-dyn} \quad \tau \]
apply (induct rule: igtlc-wt.induct)
apply clarify apply (rule conjI) apply force
apply (simp add: no-dyn-lookup)
apply clarify apply (rule conjI) apply force
apply (simp add: no-dyn-lookup)
apply (case-tac c) apply simp apply simp apply simp apply simp apply simp
apply clarify apply (rule conjI)
apply clarify apply (erule impE) apply simp add: no-dyn-fun
apply (case-tac no-dyn \(\tau_1\)) apply simp apply simp
apply clarify
apply (erule impE) apply simp apply (case-tac no-dyn \(\tau_1\))
apply simp apply simp apply simp apply simp apply simp apply simp
apply clarify
proof –
fix S \quad \Gamma \quad n0 \quad n1 \quad e \quad \tau_1 \quad n2 \quad e' \quad \tau_2
assume st12b: S \vdash \tau_1 \simeq \tau_2 \Rightarrow UVarT n2 and ndg: no-dyn \quad \Gamma
and nda: no-dyn (\text{App e e'})
and IH1: no-dyn \quad \Gamma \quad \land \quad \text{no-dyn} \quad e \Rightarrow S; \Gamma \vdash e : \tau_1 \land \text{no-dyn} \quad \tau_1
and IH2: no-dyn \quad \Gamma \quad \land \quad \text{no-dyn} \quad e' \Rightarrow S; \Gamma \vdash e' : \tau_2 \land \text{no-dyn} \quad \tau_2
from ndg nda IH1 have wte: S; \Gamma \vdash e : \tau_1 by auto
from ndg nda IH1 have ndt1: no-dyn \quad \tau_1 by auto
from ndg nda IH2 have wtep: S; \Gamma \vdash e' : \tau_2 apply auto apply (case-tac no-dyn \(\epsilon\))
apply simp apply simp done
from ndg nda IH2 have ndt2: no-dyn \quad \tau_2 apply auto apply (case-tac no-dyn \(\epsilon\))
apply simp apply simp done
from ndt2 have ndt2b: no-dyn \quad (\text{\(\tau_2\} \Rightarrow UVarT n2) \text{ by simp}
from st12b ndt1 ndt2b have st1t2b: $S \tau_1 = S (\tau_2 \rightarrow UVarT n2)$ 
by (rule conseq-no-dyn-equal)
from wte wtep st1t2b show $S\Gamma \vdash \text{App } e \ e' : UVarT n2 \land \text{no-dyn } (UVarT n2)$ 
by force
qed

References


