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: http://scholar.colorado.edu/csci_techreports

Recommended Citation
http://scholar.colorado.edu/csci_techreports/970

This Technical Report is brought to you for free and open access by Computer Science at CU Scholar. It has been accepted for inclusion in Computer Science Technical Reports by an authorized administrator of CU Scholar. For more information, please contact cuscholaradmin@colorado.edu.
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.
# Contents

1 Introduction ........................................ 3
2 Review of Gradual Typing and Inference ........ 4
3 Exploration of the Design Space ................. 8
4 A Type System for $\lambda^{\alpha}_{\omega}$ ............ 10
   4.1 The Consistent-equal and Consistent-less Judgments 11
   4.2 The Definition of the Type System ................ 13
   4.3 Properties of the Type System for $\lambda^{\alpha}_{\omega}$ 14
5 A Type Inference Algorithm for $\lambda^{\alpha}_{\omega}$ ... 15
   5.1 Constraint Generation .......................... 16
   5.2 Constraint Solver .............................. 16
   5.3 Properties of the inference algorithm .......... 19
6 Related Work ....................................... 21
7 Conclusion .......................................... 22
A Isabelle Formalization ............................ 22
   A.1 Syntax and Auxilliary Functions ............... 22
   A.1.1 Auxilliary Functions ....................... 23
   A.1.2 Properties of Auxilliary Functions .......... 25
   A.2 The Simply Typed Lambda Calculus ............ 26
   A.3 Choosing Fresh Variables ...................... 31
   A.4 The Consistency and Less Informative Relations 32
   A.5 The Gradual Type System ....................... 34
   A.6 Consistent-equal and Consistent-less .......... 34
   A.6.1 Properties of Consistent-equal/less .......... 34
   A.7 The Gradual Type System with Type Variables 38
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 almost 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.

```ml
let incr x = x + 1
let a:int = 1
incr a
```

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 coercions 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 → int) and a parameter l with type int list.

```ml
let rec map (f:int→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 *)
```
The function call \( \text{map} \ \text{incr} [1; 2; 3] \) is allowed by the gradual type system, even though the type of the argument \( \text{incr} \ (\ ? \to \text{int}) \) differs from the type of the parameter \( (\text{int} \to \text{int}) \). 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, \( \text{map} \ a [1; 2; 3] \) elicits a compile-time error because argument \( a \) has type \( \text{int} \) 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 \( \sim \) 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.

\[
\begin{align*}
\text{int} & \sim \text{int} \\
\text{int} & \not\sim \text{bool} \\
? & \sim ? \\
\text{int} \to ? & \sim ? \to \text{int} \\
\text{int} \to ? & \not\sim \text{int} \to \text{bool} \\
\text{int} \to ? & \not\sim \text{bool} \\
\text{int} & \not\sim \text{bool} \\
\text{int} \to ? & \not\sim \text{int} \to ? \\
\text{int} \to ? & \not\sim \text{int} \to \text{bool}
\end{align*}
\]

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

**Type Consistency**

\[
\begin{align*}
(C_{\text{Refl}}) & \quad \tau \sim \tau \\
(C_{\text{Fun}}) & \quad \frac{\tau_1 \sim \tau_2, \rho_1 \sim \rho_2}{\tau_1 \to \rho_1 \sim \tau_2 \to \rho_2} \\
(C_{\text{DR}}) & \quad \frac{\tau \sim ?}{? \sim ?} \\
(C_{\text{DL}}) & \quad \frac{? \sim \tau}{? \sim \tau}
\end{align*}
\]

The syntax of the gradually typed lambda calculus \( (\lambda^? \rightarrow) \) 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 \( (\text{App}2) \) 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 \( \lambda^? \rightarrow \)**

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

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 \( \text{int} \rightarrow \text{int} \).

```ocaml
# let f x = x + 1;;
val f : int \rightarrow int = \langle \ast \rangle
```

The type inference problem is formulated by attaching a type variable, an 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.

```ocaml
let f α x β = (x γ + δ 1 χ) ρ
```

The inference algorithm models the rules of a type system as equations that must hold between the type variables. For example, the type \( β \) of the parameter \( x \) must be equal to the type \( γ \) 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 \( γ \) and \( χ \), and the return type of \( + \), also \( \text{int} \), must be equal to \( ρ \). Ultimately, the type \( α \) of \( f \) must be equal to the function type \( β \rightarrow ρ \) formed from the parameter type \( β \) and the return type \( ρ \). 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 \( τ_1 = τ_2 \), we have \( S(τ_1) = S(τ_2) \).

A natural setting in which to formalize type inference is the simply typed lambda calculus with type variables (\( \lambda^\alpha_\tau \)). The syntax is similar to \( \lambda_\tau \), 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 \( \lambda^\alpha_\tau \) is well-typed in environment \( Γ \) if there is a substitution \( S \) and a type \( τ \) such that \( S(Γ) ⊢ S(e) : τ \).

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

An inference algorithm for \( \lambda^\alpha_\tau \) 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 \( \lambda^\alpha_\tau \) 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].
\[ \Gamma(x) = \tau_1 \quad \Gamma \vdash x : \tau_1 \quad \Gamma \vdash c : \text{typeof}(c) \]
\[ \Gamma \vdash e_1 : \tau_1 \to \tau_2 \quad \Gamma \vdash e_2 : \tau_1 \]
\[ \Gamma(x \mapsto \tau_1) \vdash e : \tau_2 \]
\[ \Gamma \vdash \lambda x : \tau_1. e : \tau_1 \to \tau_2 \]

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

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

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 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 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 \( S(\tau) = \tau_1 \to \tau_2 \) then \( S(\tau_2) = \tau_2 \).

**Proof.** We have \( \tau_1 \to \tau_2 = S(\tau) = S(S(\tau)) = S(\tau_1 \to \tau_2) = S(\tau_1) \to S(\tau_2) \). 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 $S; \Gamma \vdash e : \tau$. \qed

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.

```plaintext
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 \( g \ x \). 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.

```plaintext
let f (x : int) (g : ? → ?) =
g x
```

From the function application, the inference algorithm would deduce \(? → ? = \text{int} → \beta\), where \( \beta \) is a fresh variable representing the result type of the application \( g \ x \). 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 \( \lambda_\alpha \), saying that a program is well typed if there is some substitution that makes the program well typed in \( \lambda_\alpha \). 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 \( \lambda_\alpha \) (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 \text{int} and a function.

```plaintext
let f (g : \alpha) = g 1
f 1
```

Applying the substitution \( \{ \alpha \mapsto ? \} \) produces a program that is well-typed in \( \lambda_\alpha \).

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.

```plaintext
let x : \alpha = 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 \( f(x:?) = \)
\[
\text{let } y : \alpha = x \text{ in } y
\]

Here, the only appropriate solution for \( \alpha \) 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 \( \alpha \). Suppose we choose \( \alpha = \text{int} \). This type checks in \( \lambda ? \to \text{int} \) because \( \text{int} \) 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 \( \lambda ?^\alpha \)

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**

\[
\begin{align*}
\text{(LID)} & : ? \sqsubseteq \tau \\
\text{(LIREFL)} & : \tau \sqsubseteq \tau \\
\text{(LIFUN)} & : \frac{\tau_1 \sqsubseteq \tau_3 \quad \tau_2 \sqsubseteq \tau_4}{\tau_1 \to \tau_2 \sqsubseteq \tau_3 \to \tau_4}
\end{align*}
\]

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.

\[
\begin{align*}
\text{let } f(g:\alpha) &= g \ 1 \\
f \ 1
\end{align*}
\]

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 \( \text{int} \).

\[
\begin{align*}
\text{let } x:\alpha &= x + 1
\end{align*}
\]

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 \( S \vdash \tau \simeq \tau \) and consistent-less, which has the form \( S \vdash \tau \subseteq \tau \). The two judgments are defined in Figure 5. The consistent-equal judgment is similar to the type consistency relation \( \simeq \) 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 \( \subseteq \) 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 \( S \vdash \tau \subseteq \tau \) 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.

\[
S \vdash \text{int} \to \alpha \simeq ? \to (\beta \to (\text{int} \to ?))
\]

What choices for \( S \) satisfies the above constraint? Applying the inverse of the (CEFUn) rule we have

\[
S \vdash \text{int} \simeq ?, \quad S \vdash \alpha \simeq \beta \to (\text{int} \to ?)
\]

The first constraint is satisfied by any substitution using rule (CDDR), but the second constraint is satisfied when

\[
S \vdash \beta \to (\text{int} \to ?) \subseteq S(\alpha)
\]
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 \( \models \cdot \leadsto \cdot \) 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 \( S \models \alpha \leadsto \beta \) then \( S(\alpha) = S(\beta) \). This is why \( \{\alpha \mapsto \text{int}\} \) is a solution for the following program but \( \{\alpha \mapsto ?\} \) is not.

```plaintext
let f(x:α) =
  let y:β = x in y + 1
```

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

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

2. Suppose \( \tau_1 \) and \( \tau_3 \) do not contain \( ? \)s. Then \( S \models \tau_1 \subseteq \tau_2 \) and \( S \models \tau_1 \leadsto \tau_3 \) 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 \( \tau_1 = \tau_{11} \rightarrow \tau_{12} \), \( \tau_{11} \simeq S(\tau_2) \), 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 \( \tau_1 \simeq \tau_2 \).

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 (\( \lambda^?_\alpha \)). As in \( \lambda^\alpha \), 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 \( \lambda^?_\alpha \) with the judgment \( S; \Gamma \vdash g : \tau \), shown in Figure 6. The crux of the type system is the application rule (GApp). We considered a couple of alternatives before arriving at this rule. First we tried to borrow the (SApp) rule of \( \lambda^\alpha \) (Figure 4) but replace \( S(\tau_1) = S(\tau_2 \rightarrow \tau_3) \) with \( S \vdash \tau_1 \simeq \tau_2 \rightarrow \tau_3 \):

\[
\begin{align*}
S; \Gamma \vdash g_1 : \tau_1 & \quad S; \Gamma \vdash g_2 : \tau_2 & \quad S \vdash \tau_1 \simeq \tau_2 \rightarrow \tau_3 \\
S; \Gamma \vdash g_1 e_1 : \tau_3 & \quad S; \Gamma \vdash g_2 e_2 : \tau_3
\end{align*}
\]

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

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

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

\[
\begin{align*}
\Gamma_0 &= \{ f : \text{int} \rightarrow \text{int} \} \\
\Gamma_1 &= \Gamma_0(g \mapsto (\text{int} \rightarrow \text{bool}))
\end{align*}
\]

Then we have

\[
\begin{align*}
\{\} ; \Gamma_1 \vdash g : \text{int} \rightarrow \text{bool} \\
\{\} ; \Gamma_1 \vdash g_1 : \text{int} \\
\{\} ; \Gamma_0 \vdash (f \ (g \ 1)) : \text{int} \\
\{\} ; \Gamma_0 \vdash (\lambda g : \text{int} \rightarrow \text{bool}. f \ (g \ 1)) : \text{int}
\end{align*}
\]

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

\[
\begin{align*}
S; \Gamma \vdash g_1 e_1 : ? & \quad S; \Gamma \vdash g_2 e_2 : \tau \\
S; \Gamma \vdash g_1 e_1 e_2 : ? & \quad S; \Gamma \vdash g_2 e_2 : \tau \\
S; \Gamma \vdash g_1 e_1 : \tau_1 \rightarrow \tau_3 & \quad S; \Gamma \vdash g_2 e_2 : \tau_2 & \quad S \vdash \tau_1 \simeq \tau_2
\end{align*}
\]
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 \((G\text{App})\) rule as follows.

\[
(G\text{App}) \quad S; \Gamma \vdash g e_1 : \tau_1 \quad S; \Gamma \vdash g e_2 : \tau_2 \quad S \models \tau_1 \simeq \tau_2 \rightarrow \beta \quad (\beta \text{ fresh}) \\
S; \Gamma \vdash g e_1 e_2 : \beta
\]

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

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

we have the constraint set

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

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

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

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

**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 \(\tau' \sqsubseteq S(\tau)\).
Proof. The proof is by induction on the typing derivations.

The type system for $\lambda^{?=\alpha}_\alpha$ 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 $\lambda^\alpha_\alpha$. (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: $(\lambda x : \alpha. x) 1$.

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

**Theorem 4.** If $e \in \lambda^{?=\alpha}_\alpha$ and $(\forall \alpha. \Gamma(\alpha) = \tau \implies \tau \in \lambda^\alpha_\alpha)$ then $S; \Gamma \vdash_g e : \tau$ implies $S; \Gamma \vdash e : \tau$ and $\tau \in \lambda^\alpha_\alpha$.

**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 $\lambda^{?=\alpha}_\alpha$

The inference algorithm we develop for $\lambda^{?=\alpha}_\alpha$ follows a similar outline to that of the algorithm for $\lambda^\alpha_\alpha$ 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 $\{ \alpha \rightarrow \alpha \simeq ? \rightarrow \text{int} \}$. The unification algorithm would first unify $\alpha$ and $?$ and substitute $?$ for $\alpha$ on the other side of the $\rightarrow$. 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 $\text{GApp}$ rule becomes a generated constraint on the $\text{CApp}$ 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.

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

We generate the following constraints from this program.

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

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. \hfill $\square$

5.2 Constraint Solver

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

$$\begin{align*}
u_{\alpha} & \rightarrow u \rightarrow \text{w} \rightarrow \text{v} \rightarrow \text{x}_{\text{int}} \rightarrow \text{w} \rightarrow u \rightarrow v_{\alpha} \rightarrow x_{\text{int}}
\end{align*}$$
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 $\text{stye}$ 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 $\text{stye}$ of a node as a subscript, such as $u_{v \rightarrow w}$ and $x_{\text{int}}$. Also, when the identity of a node is not important we sometimes just write the $\text{stye}$ 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 $\text{true}$ 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 $\text{solve}$ algorithm is in Figure 8. We defer discussion of the $\text{copy}$. $\text{dyn}$ 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 $\text{?}$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 $\text{var}$) is overridden by anything else. To handle $\text{?}$s, we use the rules that $\text{?}$ overrides $\text{var}$ but is overridden by anything else. Thus, $\text{?}$ 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 ($\text{copy}$. $\text{dyn}$ 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 $\text{?}$ type. In both cases the node labeled int overrides $\text{?}$ 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 $\text{?} \simeq v_1 \rightarrow v_2$, deserves some explanation. Consider the program $(\lambda f : \text{?}. \, \lambda x : \alpha. \, f x)$. 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 $\text{?} \rightarrow \text{?}$, so in some sense, we really should have the constraint $\text{?} \rightarrow ? \simeq \alpha \rightarrow \beta$. To simulate this in the algorithm we insert two constraints: $\text{?} \simeq v_1$ and $\text{?} \simeq v_2$. Now, some care must be taken to prevent infinite loops. Consider the constraint $\text{?} \simeq v$ where $\text{stye}(v) = v \rightarrow v$. 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 $C$.empty() do
\[
x \simeq y := C.\text{pop}()
u := \text{find}(x); v := \text{find}(y)
\]
if $u \neq v$ then
\[
(u, v, f) := \text{order}(u, v)
\]
union($u$, $v$, $f$)
case stype($u$) $\simeq$ stype($v$) of
\[
u_1 \rightarrow u_2 \simeq v_1 \rightarrow v_2 \Rightarrow (\star \text{ case 1 } \star)
\]
$C$.push($u_1, v_1$); $C$.push($u_2, v_2$)
\mid $u_1 \rightarrow u_2 \simeq ? \Rightarrow (\star \text{ case 2 } \star)$
if $u$.contains\_vars then
\[
u.\text{contains\_vars} := \text{false}
\]
$w_1 = \text{new\_vertex}(\text{stype=}, \text{contains\_vars=false})$
\[
w_2 = \text{new\_vertex}(\text{stype=}, \text{contains\_vars=false})
\]
$C$.push($w_1 \simeq u_1$); $C$.push($w_2 \simeq u_2$)
\mid $\tau \simeq \text{var} \mid \tau \simeq ? \Rightarrow (\star \text{ pass, case 3 and 4 } \star)$
\mid $\gamma \simeq \gamma \Rightarrow (\star \text{ pass, case 5 } \star)$
\mid $\_ \Rightarrow \text{error: inconsistent types (\star \text{ case 6 } \star)}$
end while
\[
G = \text{the quotient of the graph by the equivalence classes}
\]
if $G$ is acyclic then
\[
\text{return } \{u \mapsto \text{stype(find}(u)) \mid u \text{ a node in the graph}\}
\]
else error
\[
\text{order}(u, v) = \text{case stype}(u) \simeq \text{stype}(v) \text{ of}
\]
\mid $\_ \Rightarrow (u, v, \text{false})$
\]
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 \texttt{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 \texttt{f}, \texttt{g}, and \texttt{h}. The following is a simplified example that illustrates the same problem.

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

From this program we get the constraint set

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

If we forgo the \texttt{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 \texttt{copy\_dyn} conversion, the two occurrences of u? are replaced by separate nodes that can separately unify with \text{int} and \text{bool} and avoid the error. It is important that we apply the \texttt{copy\_dyn} conversion to the generated constraints and not to the original program, as that would not avoid the above problem.

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

\textbf{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

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{constraint_solver_example.png}
\caption{An example run of the constraint solver.}
\end{figure}
by $S^*$. Note that the solution $S'$ returned by 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 $S = \text{solve}(C)$ then $S^* \models C$.
2. If $S \models C$ then $\exists S'R. S' = \text{solve}(C)$ and $R \circ S'^* \subseteq S$.

*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 $R \circ S' \subseteq S$, 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 $R \circ S'^* \subseteq S$. □

**Lemma 5.** The time complexity of the 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 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 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 $(S, \tau) = \text{infer}(\Gamma, e)$, then $S^*; \Gamma \vdash e : \tau$.
2. If $S; \Gamma \vdash e : \tau$ then there is a $S'$, $\tau'$, and $R$ such that $(S', \tau') = \text{infer}(\Gamma, e)$, $R \circ S'^* \subseteq S'$, and $R \circ S'^*(\tau') \subseteq S(\tau)$.

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

1. By the soundness of 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 solve (Lemma 4) there exists $S'$ and $R$ such that $S' = \text{solve}(C)$ and $R \circ S'^* \subseteq S$. 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 $O(n^\alpha(n))$. \hfill \square

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 downcasts. 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. Sick 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

**types** \( \text{name} = \text{nat} \)

**datatype** \( \text{ty} = \)
- \( \text{UVarT name} \)
- \( \text{IntT (int)} \)
- \( \text{BoolT (bool)} \)
- \( \text{DynT (?)} \)
- \( \text{ArrowT ty ty (infixr \rightarrow 95)} \)

**datatype** \( \text{const} = \text{IntC int} \)
- \( \text{BoolC bool} \)
- \( \text{Succ} \)
- \( \text{IsZero} \)

**datatype** \( \text{expr} = \)
- \( \text{Var name} \)
- \( \text{Const const} \)
- \( \text{Lam name ty expr (\lambda-. - [53,53,53] 52)} \)
- \( \text{App expr expr} \)

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

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

**axclass** \( \text{type-struct < type} \)

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

\section*{A.1.1 Auxilliary Functions}

\textbf{constdefs} id-subst \textbf{::} subst
\textbf{id-subst-def}[simp]; id-subst \equiv \[
— domain of an association list

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

\textbf{consts}
\textit{lookup} :: ('a × 'b) list ⇒ 'a ⇒ 'b option
\textbf{primrec}
\textit{lookup} [] \_ \_ \_ = None
\textit{lookup} (kv#ls) k =
  (if \text{fst} kv = k then Some \text{snd} kv else \text{lookup} ls k)

\textbf{constdefs}
\textit{lookup-subst} :: (name × ty) list ⇒ name ⇒ ty (%)
\textit{lookup-subst S a} \equiv
  (case \text{lookup} S a of None ⇒ UVarT a | Some \text{t} ⇒ \text{t})

\textbf{consts}
\textit{app-subst} :: [subst, 'a::type-struct] ⇒ 'a::type-struct ($)
\textbf{syntax (latex)}
\textit{app-subst} :: [subst, 'a::type-struct] ⇒ 'a::type-struct ()

\textbf{primrec} (\textit{app-subst-ty})
\textit{S} (UVarT a) = \% S a
\textit{S} (IntT) = (IntT)
\textit{S} (BoolT) = (BoolT)
\textit{subst-fun}: \textit{S} (t₁ → t₂) = (\textit{S} t₁) → (\textit{S} t₂)
\textit{S} (? ) = (? )

\textbf{primrec} (\textit{app-subst-list})
\textit{S} [] = []
\textit{S} (x#xs) = (\textit{S} x)#(\textit{S} xs)

\textbf{defs (overloaded)}
\textit{app-subst-pair}: \textit{S} p \equiv (\text{fst} p, \textit{S} (\text{snd} p))

\textbf{primrec} (\textit{app-subst-expr})
\textit{subst-var}: \textit{S} (Var x) = (Var x)
\textit{S} (Const c) = (Const c)
\textit{subst-abs}: \textit{S} (λx::τ. e) = (λx::\textit{S} τ. \textit{S} e)
\textit{S} (App e₁ e₂) = (App (\textit{S} e₁) (\textit{S} e₂))

\textbf{primrec} (\textit{app-subst-option})
\textit{app-subst} S None = None
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 \ \lambda x.))

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

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

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

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

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

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

defs (overloaded)
FTV-pair[simp]: FTV p \equiv FTV (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\}

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

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

primrec (no-dyn-expr)
no-dyn (Var x) = True
no-dyn (Const c) = True
no-dyn (\lambda \ x:\tau. \ e) = (if no-dyn \tau then no-dyn e else False)
no-dyn (App e1 e2) = (if no-dyn e1 then no-dyn e2 else False)
defs (overloaded)

\begin{align*}
\text{no-dyn-fun: no-dyn } \Gamma & \equiv (\forall \; x \; a. \; \Gamma \; x = a \; \longrightarrow \; \text{no-dyn } a) \\
\text{primrec (no-dyn-option)} \\
\text{no-dyn None} &= \text{True} \\
\text{no-dyn (Some } \tau \text{)} &= \text{no-dyn } \tau 
\end{align*}

defs (overloaded)

\begin{align*}
\text{no-dyn-pair[simp]: no-dyn } p & \equiv \text{no-dyn } (\text{snd } p) \\
\text{primrec (no-dyn-list)} \\
\text{no-dyn } \text{[]} & = \text{True} \\
\text{no-dyn } (a \# \text{ls}) & = (\text{if no-dyn } a \text{ then no-dyn } \text{ls else False}) 
\end{align*}

constdefs

\begin{align*}
\text{idempotent } :: \, \text{subst } \Rightarrow \, \text{bool} \\
\text{idempotent } S & \equiv S (\% \; S) = \% \; S 
\end{align*}

A.1.2 Properties of Auxiliary Functions

\begin{enumerate}
\item \textbf{lemma finite-ftv-ty[intro!]:} finite \((FTV \; (\tau::ty))\)
\item apply (induct \(\tau\)) by auto
\item \textbf{lemma finite-ftv-expr[intro!]:} finite \((FTV \; (e::expr))\)
\item apply (induct \(e\)) by auto
\item \textbf{lemma finite-ftv-subst[intro!]:} finite \((FTV \; (S::subst))\)
\item apply (induct \(S\)) by auto
\item \textbf{lemma id-id[simp]:} $\text{id-subst } (\tau::ty) = \tau$ apply (induct \(\tau\))
\item using lookup-subst-def by auto
\item \textbf{lemma closed-subst-id:} \(FTV \; \tau = \{\} \implies S \; \tau = (\tau::ty)\)
\item apply (induct \(\tau\)) by auto
\item \textbf{lemma idempotent-ty[rule-format]:} \(\forall \; S. \; \text{idempotent } S \longrightarrow S \; (\% \; S \; t) = S \; (t::ty)\)
\item apply (induct \(t\)) defer apply simp apply simp apply simp apply simp apply simp
\item proof –
\item fix \(n::\text{nat}\)
\item show \(\forall \; S. \; \text{idempotent } S \longrightarrow S \; (\% \; S \; (UVarT \; n)) = S \; (UVarT \; n)\)
\item proof clarify
\item fix \(S\) assume id: idempotent \(S\)
\item have \(S \; (\% \; S \; (UVarT \; n)) = S \; (\% \; S \; n)\) by simp
\item also have \(\ldots = (S \; (\% \; S)) \; n\) by (simp add: app-subst-fan)
\item also from id have \(\ldots = \% \; S \; n\) by (simp add: idempotent-def)
\item also have \(\ldots = S \; (UVarT \; n)\) by simp
\item finally show \(S \; (\% \; S \; (UVarT \; n)) = S \; (UVarT \; n)\) by blast
\item qed
\item qed
\item \textbf{lemma ftv-dom-id[rule-format]:} \(\forall \; S. \; (\forall \; a. \; a \in FTV \; \tau \longrightarrow \% \; S \; a = UVarT \; a) = (S \; \tau = (\tau::ty))\)
\item apply (induct \(\tau\)) by auto
\item proof
\item – This is Lemma 2 of the paper
\item \textbf{lemma t1tot2eqSt-implies-t2eqSt2[rule-format]:}
\end{enumerate}
lemma \textit{Steqt1tot2-implies-st2eqt2}:
\begin{align*}
\text{idempotent } S \land (S \tau = \tau_1 \rightarrow \tau_2) \rightarrow \tau_2 = S \tau_2
\end{align*}
proof 
- fix \(a\)
assume \(\text{tmp: idempotent } S \land S (UVarT a) = \tau_1 \rightarrow \tau_2\)
from \(\text{tmp have idems: idempotent } S \text{ by simp}\)
from \(\text{idems have sstt: } S (S (UVarT a)) = (S (S (UVarT a)))\)
by (rule idempotent-ty)
with \(\text{tmp sstt have sneqt1tol2: } (S (S (UVarT a))) = S \tau_1 \rightarrow S \tau_2 \text{ by simp}\)
with \(\text{tmp show } \tau_2 = S \tau_2 \text{ by simp}\)
next
- fix \(ty1 ty2\)
assume \(\text{styc: idempotent } S \land S ty1 = \tau_1 \land S ty2 = \tau_2\)
hence \(\text{idempotent } S \text{ by simp}\)
hence \(S (S ty2) = S ty2 \text{ by (rule idempotent-ty)}\)
with \(\text{styc show } \tau_2 = S \tau_2 \text{ by simp}\)
qed

\textbf{A.2 The Simply Typed Lambda Calculus}

\textbf{consts} \(\text{TypeOf :: const } \Rightarrow ty\)

\textbf{primrec}
\(\text{TypeOf (IntC } n) = \text{IntT}\)
\(\text{TypeOf (BoolC } b) = \text{BoolT}\)
\(\text{TypeOf Succ = IntT } \rightarrow \text{IntT}\)
\(\text{TypeOf IsZero = IntT } \rightarrow \text{BoolT}\)

\textbf{inductive stlc-wt :: env } \Rightarrow \text{expr } \Rightarrow ty \Rightarrow \text{bool } (-\vdash - : - [52,52,52] 51)\)
\textit{where}
\begin{align*}
\text{Var[introl]: } \begin{cases} 
\text{lookup } \Gamma x = \text{Some } \tau \implies \Gamma \vdash \text{Var } x : \tau \\
\text{Const[introl]: } \Gamma \vdash \text{Const } c : \text{TypeOf } c \\
\text{Abs[introl]: } \begin{cases} 
(x,\tau_1) \# \Gamma \vdash e : \tau_2 \implies \Gamma \vdash (\lambda x : \tau_1. e) : \tau_1 \rightarrow \tau_2 \\
\text{App[introl]: } \begin{cases} 
\Gamma \vdash e : \tau_1 \rightarrow \tau_2; \Gamma \vdash e' : \tau_1 \\
\implies \Gamma \vdash (\text{App } e e') : \tau_2 \\
\end{cases}
\end{cases}
\end{cases}
\end{align*}

\textbf{inductive stlc-wt :: subst[env] } \Rightarrow \text{[expr,ty] } \Rightarrow \text{bool } (-\vdash - : - [52,52,52,52] 51)\)
\textit{where}
\begin{align*}
\text{SVar[introl]: } \begin{cases} 
\text{lookup } \Gamma x = \text{Some } \tau \implies S;\Gamma \vdash \text{Var } x : \tau \\
\text{SConst[introl]: } \tau = \text{TypeOf } c \Rightarrow S;\Gamma \vdash \text{Const } c : \tau \\
\text{SAbs[introl]: } \begin{cases} 
S(x,\tau_1) \# \Gamma \vdash e : \tau_2 \implies S;\Gamma \vdash (\lambda x : \tau_1. e) : \tau_1 \rightarrow \tau_2 \\
\end{cases}
\end{cases}
\end{align*}
lemma ex-t[rule-format]: \forall \ S x. \ lookup \ (\$S::\text{subst}) \ (\Gamma::\text{env}) \ x = \text{Some} \ \tau \longrightarrow \\
(\exists \ \tau'. \ lookup \ \Gamma' \ x = \text{Some} \ \tau' \land \$S \ \tau' = \tau) \\
apply \ (\text{induct} \ \Gamma') \\
apply \ \text{smp} \\
apply \ \text{clarify} \ apply \ (\text{simp add: \ app-subst-pair}) \\
apply \ (\text{case-tac} \ a = x) \ apply \ \text{smp} \\
apply \ \text{auto} \\
\text{done} \\

lemma idem-ftvst-impl: \\
\forall \ S a. \ \text{idempotent} \ S \land a \in \text{FTV} \ (\$S \ (\tau::\text{ty})) \longrightarrow \ %S a = UVarT a \\
apply \ (\text{induct} \ \tau) \\
defer apply \ \text{smp} \ apply \ \text{smp} \ apply \ \text{smp} \ apply \ \text{smp} \ apply \ \text{smp} \ apply \ blast \\
defer apply \ \text{clarify} 
proof – 
fix \ b \ S \ a 
assume \ ids: \ \text{idempotent} \ S \ \text{and} \ aftv: \ a \in \text{FTV} \ (\$S \ (UVarT b)) 
from \ ids \ have \ $S \ (\$S \ (UVarT b)) = $S \ (UVarT b) \ \text{by} \ (\text{rule \ idempotent-ty}) 
hence \ \forall \ a. \ a \in \text{FTV} \ (\$S \ (UVarT b)) \longrightarrow \ %S a = UVarT a \ \text{using} \ \text{ftv-dom-id} \ \text{by} \ \text{blast} 
with \ aftv \ show \ %S a = UVarT a \ \text{by} \ \text{smp} 
qed 

lemma idem-ftvst: \\
[ idempotent \ S; a \in \text{FTV} \ (\$S \ (\tau::\text{ty})) ] \longrightarrow \ %S a = UVarT a \\
using \ idem-ftvst-impl \ \text{by} \ \text{blast} 

lemma ftv-wt-sub-impl: \ \Gamma' \vdash \ e' : \tau \longrightarrow \\
\forall \ \tau. \ \text{idempotent} \ S \land \ e' \in \text{FTV} \ \tau \longrightarrow \ %S a = UVarT a \\
apply \ (\text{induct \ rule: \ stlc-wt.induct}) 
defer apply \ (\text{case-tac} \ c) \ apply \ \text{force} \ apply \ \text{force} \ apply \ \text{force} \ apply \ \text{force} \ apply \ \text{force} 
proof clarify apply \ (\text{case-tac} \ ca) \ apply \ \text{force} \ apply \ \text{force} \ apply \ \text{force} \ apply \ \text{prefer} \ 2 \ apply \ \text{force} 
apply \ \text{smp} \ apply \ (\text{erule-tac} \ x=(x,\tau_1)\#\Gamma' \ \text{in} \ \text{allE}) 
apply \ (\text{erule-tac} \ x=\text{expr} \ \text{in} \ \text{allE}) 
apply \ (\text{erule-tac} \ x=S \ \text{in} \ \text{allE}) \ apply \ (\text{erule \ impE}) \ apply \ \text{smp} 
apply \ (\text{smp \ add: \ app-subst-pair}) \ apply \ (\text{smp \ add: \ idempotent-ty}) 
apply \ \text{clarify} \ apply \ (\text{erule \ disjE}) \ apply \ \text{smp} 
using \ idem-ftvst \ apply \ \text{smp} \ apply \ \text{smp} 
apply \ \text{clarify} \ apply \ (\text{case-tac} \ ca) \ apply \ \text{force} \ apply \ \text{force} \ apply \ \text{force} \ apply \ \text{force} 
apply \ (\text{erule-tac} \ x=\Gamma' \ \text{in} \ \text{allE}) \ apply \ (\text{erule-tac} \ x=\Gamma' \ \text{in} \ \text{allE}) 
apply \ (\text{erule-tac} \ x=\text{expr} \ \text{in} \ \text{allE}) \ apply \ (\text{erule-tac} \ x=\text{expr} \ \text{in} \ \text{allE}) 
apply \ (\text{erule-tac} \ x=S \ \text{in} \ \text{allE}) \ apply \ (\text{erule-tac} \ x=S \ \text{in} \ \text{allE}) 
apply \ (\text{erule \ impE}) \ apply \ (\text{smp \ add: \ app-subst-fun}) 
apply \ \text{smp} 
apply \ \text{clarify} 
proof – 
fix \ \Gamma \ x \ \text{and} \ \tau::\text{ty} \ \text{and} \ \Gamma' \ e \ \text{and} \ S::\text{subst} \ \text{and} \ a 
assume \ sgx: \ lookup \ (\$S \ \Gamma') \ x = \text{Some} \ \tau \ \text{and} \ \text{idem} \ S 
and \ xgx: \ \text{Var} \ x = $S \ e \ \text{and} \ aft: \ a \in \text{FTV} \ \tau 
from \ sgx \ have \ X: \ \exists \ \tau'. \ lookup \ \Gamma' \ x = \text{Some} \ \tau' \land \$S \ \tau' = \tau \ \text{by} \ (\text{rule \ ex-t}) 
from \ X \ obtain \ \tau' \ \text{where} \ \text{gpx:} \ \text{lookup} \ \Gamma' \ x = \text{Some} \ \tau' \ \text{and} \ \text{stp:} \ $S \ \tau' = \tau \ \text{by} \ \text{blast}
from afst stp have afst: a ∈ FTV ($S \tau$) by simp
from ids afst show % S a = UVarT a by (rule idem-ftvst)
qed

lemma ftv-wt-sub: [$S \Gamma \vdash S e : \tau; \text{idempotent } S$]
⇒ (∀ a. a ∈ FTV τ → %S a = UVarT a)
using ftv-wt-sub-impl apply blast done

— Lemma 1 of the paper
lemma ewt-ewSt:
assumes idems: idempotent S and ewt: $S \Gamma \vdash S e : \tau$
shows $S S \Gamma \vdash S e : S \tau$
proof –
from ewt idems have (∀ a. a ∈ FTV τ → %S a = UVarT a) by (rule ftv-wt-sub)
hence $S S \tau = \tau$ using ftv-dom-id by blast
thus $S S \Gamma \vdash S e : S \tau$ by simp
qed

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

lemma stlc-implies-istlc-impl:
$\Gamma \vdash e' : \tau' \Rightarrow$
(∀ e S τ. idempotent S ∧ $\Gamma' = S S \Gamma \wedge e' = S e \wedge \tau' = (S S \tau$)
⇒ (∃ τ". (S;Γ + e : τ" ∧ $S S \tau" = \tau'$)))
apply (induct rule: stlc-wt.induct)
apply clarify defer apply clarify defer apply clarify defer apply clarify defer
proof –
fix $x \tau$ and $\Gamma'::\text{env}$ and $e::\text{expr}$ and $S::\text{subst}$ and $\tau'$
assume $\text{sgx} :: \text{lookup} (S S \Gamma') x = \text{Some } (S S \tau')$ and idems: idempotent S
and $\text{vx} :: \text{Var } x = S S e$
from $\text{sgx ex-I obtain } \tau"$ where $\text{lxz} :: \text{lookup } \Gamma' x = \text{Some } \tau"$
and $\text{sst: }$ $S S \tau" = S S \tau'$ by blast
from $\text{vxe lxz sst show }$ $\exists \tau"$. $S;\Gamma' + e : \tau" \wedge S S \tau" = S S \tau'$
apply (case-tac $c::\text{expr}$) apply (rule-tac $x=\tau"$ in exI) by auto
next
fix $S \Gamma' e S \tau$
assume idempotent S and $\text{Const } c = S S e$ and $\text{TypeOf } c = S S \tau$
thus $\exists \tau". S;\Gamma' + e : \tau" \wedge S S \tau" = \text{TypeOf } c$
apply (rule-tac $x=\text{TypeOf } c$ in exI)
apply (simp add: idempotent-ty)
apply (case-tac $c::\text{expr}$) apply auto done
next
fix $x \tau_1 \Gamma e \tau_2 \Gamma' ea S \tau$
assume $IH1: \forall \Gamma ea Sa \tau$. 

28
idempotent $Sa \land$
\[(x, \tau_1) \# S \Gamma' = S \gamma \land e = S \gamma \land \tau_2 = S \gamma \tau \rightarrow\]
\[(\exists \tau'''. \forall \gamma \Gamma' \vdash e : \tau''' \land \exists S \gamma \tau'' = \tau_2)\]
and ids: idempotent $S$ and le: $\lambda x : \tau_1, e = S \gamma \land \tau_2 = S \gamma \tau$ from le obtain $t b$ where $ea : \lambda x : t, b$ and $t1st : \tau_1 = S S t$
and esb: $e = S b \ apply (case-tac ea::expr) \ apply auto \ done$
from ids $t1st$ have $t2st : \tau_2 = S S \tau_2 \ using \ Steq11to10-implies-12eqSt2 \ by \ blast$
from ids $IH1$ $t1st \ esb$
have $X : \exists \tau'''. \ S \gamma x t \# \Gamma' \vdash b : \tau''' \land S S \tau'' = \tau_2$
apply auto apply (erule-tac $x=(x,t)\#\Gamma'\ in \ allE$)
  apply (erule-tac $x=b \ in \ allE$)
  apply (erule-tac $x=S \ in \ allE$)
apply (erule-tac $x=\tau_2 \ in \ allE$) \ apply auto
apply (simp add: app-subst-pair) using $t2st$ apply simp \ done
from $X$ obtain $t2$ where $wtb: S \gamma x t \# \Gamma' \vdash b : t2$ and $st2t2 : S \gamma t2 = \tau_2 \ by \ blast$
from $wtb$ have $wtt: S \gamma t1 \ lam \ x : t, b : t \rightarrow t2 \ by \ blast$
with $ea$ $st2t2$ $t1st$
show $\exists \tau'''. \ S \gamma \vdash e : \tau'' \land S S \tau'' = \tau_1 \rightarrow \tau_2 \ by \ auto$
next
fix $\Gamma e \tau_1 \tau_2 e' \Gamma' ea S \tau$
assume $wte: S \gamma \vdash e : \tau_1 \rightarrow S \gamma \tau$
and $IH1: \forall \gamma \ e Sa \tau'.
  idempotent $Sa \land$
  $S \gamma \Gamma' = S \gamma \land e = S \gamma \land \tau_1 \rightarrow S \gamma \tau = S \gamma \tau' \rightarrow$
  $(\exists \tau'''. \ S \gamma \Gamma' \vdash e : \tau''' \land \exists S \gamma \tau'' = \tau_1 \rightarrow S \gamma \tau)$
and $wtep: S \gamma \vdash e' : \tau_1$
and $IH2: \forall \gamma e Sa \tau.$
  idempotent $Sa \land S \gamma \Gamma' = S \gamma \land e' = S \gamma e \land \tau_1 = S \gamma \tau \rightarrow$
  $(\exists \tau'''. \ S \gamma \Gamma' \vdash e : \tau''' \land \exists S \gamma \tau'' = \tau_1)$
and ids: idempotent $S$ and $A: App e e' = S e$ from $A$ obtain $e1 e2$ where $EA: ea = App e1 e2$ and $E: e = S S e1$
and $EP: e' = S S e2 apply (case-tac ea::expr) by auto$
from ids $wte$ $E$ have $\tau_1 \rightarrow S \gamma \tau = S S (\tau_1 \rightarrow S \gamma \tau) \ using \ ewt-teqSt \ by \ blast$
hence $t1st1 : \tau_1 = S S \tau_1 \ by \ simp$
from ids $E$ $IH1$ $t1st1$ obtain $t1$ where $wte1: S \gamma \vdash e1 : t1$
and $st1t1 : S S t1 = \tau_1 \rightarrow S S \tau$
apply auto apply (erule-tac $x=\Gamma' \ in \ allE$)
apply (erule-tac $x=e1 \ in \ allE$)
apply (erule-tac $x=S \ in \ allE$)
apply (erule-tac $x=\tau_1 \ in \ allE$)
apply auto using idempotent-ty apply simp \ done
from ids $EP$ $IH2$ obtain $t2$ where $wte2: S \gamma \vdash e2 : t2$ and $st2t1 : S S t2 = \tau_1$
apply simp apply (erule-tac $x=\Gamma' \ in \ allE$)
apply (erule-tac $x=e2 \ in \ allE$)
apply (erule-tac $x=S \ in \ allE$)
apply (erule-tac $x=\tau_1 \ in \ allE$)
apply auto using $t1st1$ apply simp \ done
from $st1t1$ $st2t1$ have eq: $S S t1 = S S (t2 \rightarrow \tau) \ by \ simp$
from $wte1$ $wte2$ $eq EA$
show $\exists \tau'''. \ S \gamma \vdash e : \tau''' \land S S \tau'' = S S \tau \ by \ auto$
qed

lemma stlc-implies-istlc-impl2:
\[ [ \ idempotent \ S; \ S \gamma \vdash S S e : S S \tau ] \implies (\exists \ \tau', \ S \gamma \vdash e : \tau' \land S S \tau' = S S \tau) \]
using stlc-implies-istlc-impl by blast
lemma stlc-implies-istlc:
  assumes ute: $S \Gamma \vdash S e : \tau$ and ids: idempotent $S$
  shows $\exists \tau'. S;\Gamma \vdash e : \tau' \land S \tau' = \tau$
proof
  from ids ute have ute2: $S \Gamma \vdash S e : S \tau$ by (rule ute-cwSt)
  from ids ute2 obtain $\tau'$ where wtep: $S;\Gamma \vdash e : \tau'$ and stst: $S \tau' = S \tau$
  using stlc-implies-istlc-impl2 by blast
  from ids ute have $S \tau = \tau$ by (rule ute-reqt)
  with wtep stst show $?thesis$ by auto
qed

lemma stlc-wt-implies-teqSt:
  assumes idems: idempotent $S$ and eut: $S \Gamma \vdash S e : \tau$
  shows $\tau = S \tau$
proof
  from eut idems have $\forall a. a \in FTV \tau \longrightarrow \%S a = UVarT a$ by (rule ftv-wt-sub)
  hence $S \tau = \tau$ 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]:
  $\forall x : \tau. S$. lookup $\Gamma x = Some \tau \longrightarrow lookup (S\Gamma) x = Some (S \tau)$
  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 $S$.subst and $\Gamma$:env and $\tau_1 \tau_2 e x$
  assume $S; (x,\tau_1) # \Gamma \vdash e : \tau_2$ and SE: $S (S (x,\tau_1) # \Gamma) \vdash S e : S \tau_2$
  have $S (S (x,\tau_1) # \Gamma) = (x, S S \tau_1) # (S \Gamma)$ by (simp add: app-subst-pair)
  with SE have $(x, S S \tau_1) # (S \Gamma) \vdash S e : S \tau_2$ by simp
  thus $S; \Gamma \vdash S (\lambda x : x. e) : S (\tau_1 \rightarrow \tau_2)$ by auto
qed

— Theorem 1 of the paper

theorem stlc-istlc-equivalent:
  (idempotent $S$ $\land S \Gamma \vdash S e : \tau$ $\longrightarrow (\exists \tau'. S;\Gamma \vdash e : \tau' \land S \tau' = \tau))$
  $\land (S;\Gamma \vdash e : \tau \longrightarrow S;\Gamma \vdash S e : S \tau$)
  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.

\[
\begin{align*}
\text{constdefs} & \quad \text{max} :: \mathbb{N} \Rightarrow \mathbb{N} \Rightarrow \mathbb{N} \\
\text{max} \ x \ y & \equiv (\text{if } x < y \ \text{then } y \ \text{else } x)
\end{align*}
\]

\[\text{declare} \ \text{max-def} [\text{simp}]\]

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.

\[\begin{align*}
\text{interpretation} \ &\ AC-max: \ AC_e [\text{max } 0 :: \mathbb{N} ] \\
\text{by unfold-locales (auto intro: add-assoc add-commute)}
\end{align*}\]

\[
\begin{align*}
\text{constdefs} & \quad \text{setmax} :: \mathbb{N} \text{ set} \Rightarrow \mathbb{N} \\
\text{setmax} \ S & \equiv \text{fold max} (\lambda x. x) 0 S
\end{align*}
\]

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.

\[\text{lemma} \ \text{max-ge}: \ \text{finite } L \implies \forall x \in L. x \leq \text{setmax } L\]

\[\begin{align*}
\text{apply} & \quad (\text{induct rule: } \text{finite-induct}) \\
\text{apply} & \quad \text{simp} \\
\text{apply} & \quad \text{clarify} \\
\text{apply} & \quad (\text{case-tac } xa = x)
\end{align*}\]

\[\text{proof} – \]

\[\text{fix } x \text{ and } F :: \mathbb{N} \text{ set and } xa \]

\[\begin{align*}
\text{assume } fF & \quad \text{finite } F \text{ and } xf: x \notin F \text{ and } xax: xa = x \\
\text{from } fF xF & \quad \text{have } mc: \text{setmax } (\text{insert } x F) = \text{max } x (\text{setmax } F) \\
\text{apply} & \quad (\text{simp only: setmax-def}) \\
\text{apply} & \quad (\text{rule AC-max.fold-insert}) \\
\text{apply} & \quad \text{auto done}
\end{align*}\]

\[\text{with } xax \text{ show } xa \leq \text{setmax } (\text{insert } x F)\]

\[\text{apply} \quad \text{clarify by simp}\]

\[\text{next}\]

\[\text{fix } x \text{ and } F :: \mathbb{N} \text{ set and } xa \]

\[\begin{align*}
\text{assume } fF & \quad \text{finite } F \text{ and } xf: x \notin F \\
\text{and } axF & \quad \forall x \in F. x \leq \text{setmax } F \\
\text{and } xxF & \quad xa \in \text{insert } x F \\
\text{and } xax & \quad xa \neq x
\end{align*}\]

\[\begin{align*}
\text{from } xax xxF & \quad \text{have } xaF: xa \in F \text{ by auto} \\
\text{with } axF & \quad \text{have } xasF: xa \leq \text{setmax } F \text{ by blast} \\
\text{from } fF xF & \quad \text{have } mc: \text{setmax } (\text{insert } x F) = \text{max } x (\text{setmax } F) \\
\text{apply} & \quad (\text{simp only: setmax-def}) \\
\text{apply} & \quad (\text{rule AC-max.fold-insert}) \\
\text{apply} & \quad \text{auto done}
\end{align*}\]

\[\text{with } xasF \text{ show } xa \leq \text{setmax } (\text{insert } x F) \text{ by auto}\]

\[\text{qed}\]

\[\text{lemma} \ \text{max-is-fresh}[\text{simp}]::\]

31
assumes \( F \): finite \( L \) shows \( \text{Suc} \ (\text{setmax} \ L) \notin L \)

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

qed

lemma greater-than-max-is-fresh: simp:
  assumes \( F \): finite \( L \) and \( I \): 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 \( A \Rightarrow \forall \ B . \text{finite} \ B \land A \subseteq B \rightarrow \text{setmax} \ A \leq \text{setmax} \ B \)
apply (induct rule: finite-induct)
apply (simp add: setmax-def)
proof clarify
  fix \( x \ F \) assume \( fF \): finite \( F \) and \( xF \): \( x \notin F \)
  and \( IH \): \( \forall B . \text{finite} \ B \land F \subseteq B \rightarrow \text{setmax} \ F \leq \text{setmax} \ B \)
  show \( \forall B . \text{finite} \ B \land \text{insert} \ x \ F \subseteq B \rightarrow \text{setmax} \ (\text{insert} \ x \ F) \leq \text{setmax} \ B \)
  proof clarify
    fix \( B \) assume \( fB \): finite \( B \) and \( xFsubB \): \( \text{insert} \ x \ F \subseteq B \)
    from \( fF xF \) have \( \text{smxF} \) : \( \text{setmax} \ (\text{insert} \ x \ F) = \max \ x \ (\text{setmax} \ F) \)
    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 \( zleB \) : \( x \leq \text{setmax} \ B \) using max-ge by blast
    from \( xFsubB \) have \( FsubB \) : \( F \subseteq B \) by auto
    from \( fB FsubB IH \) have \( \text{setmax} \ F \leq \text{setmax} \ B \) by simp
    with \( zleB \) \( \text{smxF} \) 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 ~ 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: \( \text{IntT} \sim ? \) by auto
have B: ? \( \sim \text{BoolT} \) by auto
have C: \( \neg (\text{IntT} \sim \text{BoolT}) \) by auto
from A B C show ?thesis by auto
qed

inductive less-info :: ty \Rightarrow ty \Rightarrow bool (infixl \( \sqsubseteq \))
where
LEInt[intro]: \( \text{IntT} \sqsubseteq \text{IntT} \) | 
LEBool[intro]: \( \text{BoolT} \sqsubseteq \text{BoolT} \) | 
LEVar[intro]: \( \text{UVarT} \alpha \sqsubseteq \text{UVarT} \alpha \) | 
LEFun[intro]: \( [\sigma \subseteq \tau; \sigma' \subseteq \tau'] \implies (\sigma \rightarrow \sigma') \subseteq (\tau \rightarrow \tau') \) | 
LEBottom[intro]: ? \( \sqsubseteq \tau \)

lemma less-info-refl[intro]: \( t \sqsubseteq t \)
apply (induct t) by auto

lemma less-info-transitive-impl:
\( \forall \varrho \tau. \varrho \sqsubseteq \sigma \land \sigma \sqsubseteq \tau \implies \varrho \sqsubseteq \tau \)
apply (induct \( \sigma \) ) by blast+ done

lemma less-info-transitive: \( [\varrho \subseteq \sigma; \sigma \subseteq \tau] \implies \varrho \subseteq \tau \)
using less-info-transitive-impl by blast

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]: \( \sigma \subseteq \tau \land (\forall \tau'. \tau \sim \tau' \implies \sigma \sim \tau') \)
apply (induct rule: less-info.induct)
simp
apply simp
apply simp
apply clarify
apply (erule cons-fun-any)
simp
apply (erule-tac x=t\( \) in allE)
simp
apply (erule-tac x=t\( \) in allE)
force
simp
apply blast

apply simp
apply (erule-tac x=t\( \) in allE)
simp
apply (erule-tac x=t\( \) in allE)
force
force
force
done

lemma cons-less-less: \( t_1 \sim t_2 \implies (\exists t_3. \ t_1 \sqsubseteq t_3 \land t_2 \sqsubseteq t_3) \)
apply (induct rule: consistent.induct) by blast+ done
A.5 The Gradual Type System

inductive gltc-wt :: env ⇒ [expr, ty] ⇒ bool (- ∼ - : [52,52,52] 51)
where
  WTVar[intro!]: [ lookup Γ x = Some τ ] ⇒ Γ ⊢ Var x : τ |
  WTConst[intro!]: Γ ⊢ Const c : TypeOf c |
  WTAbs[intro!]: [ (x,τ)#Γ ⊢ e : ϑ ] ⇒ Γ ⊢ (λx:τ. e) : τ → ϑ |
  WTApl1[intro!]: [ Γ ⊢ e : ?; Γ ⊢ e': τ ] ⇒ Γ ⊢ (App e e') : ? |
  WTApl2[intro!]: [ Γ ⊢ e : τ → g; Γ ⊢ e': τ'; τ' ⊑ τ ]
  ⇒ Γ ⊢ (App e e') : g

A.6 Consistent-equal and Consistent-less

inductive consistent-equal :: subst ⇒ [ty, ty] ⇒ bool (- ⊑ - : [50,50,50] 51)
and consistent-less :: subst ⇒ [ty, ty] ⇒ bool (- ⊑ - : [50,50,50] 51)
where
  CEInt[intro!]: S ⊢ IntT ⊑ IntT |
  CEBool[intro!]: S ⊢ BoolT ⊑ BoolT |
  CEDynL[intro!]: S ⊢ τ ⊑ τ |
  CEDynR[intro!]: S ⊢ τ ⊑ τ |
  CEFun[intro!]: [ S ⊢ τ ∼ τ; S ⊢ σ' ∼ τ' ] ⇒ S ⊢ (σ → σ') ∼ (τ → τ') |
  CEVarR[intro!]: S ⊢ τ ⊑ %S α ⇒ S ⊢ τ ∼ UVarT α |
  CEVarL[intro!]: S ⊢ τ ⊑ %S α ⇒ S ⊢ UVarT α ∼ τ |
  CLVar[intro!]: %S α = τ ⇒ S ⊢ UVarT α ⊑ τ |
  CLInt[intro!]: S ⊢ IntT ⊑ IntT |
  CLBool[intro!]: S ⊢ BoolT ⊑ BoolT |
  CLDynL[intro!]: S ⊢ ? ⊑ τ |
  CLDynR[intro!]: S ⊢ ? ⊑ τ |
  CLFun[intro!]: [ S ⊢ σ ⊑ τ; S ⊢ σ' ⊑ τ' ] ⇒ S ⊢ (σ → σ') ⊑ (τ → τ')

A.6.1 Properties of Consistent-equal/less

The following lemmas correspond to Proposition 1 of the paper.

lemma consless-refl: S ⊢ t ⊑ $S t apply (induct t) by auto

lemma consless-trans-impl: (S ⊢ τ1 ⊑ τ2 ⇒ True)
  ∧ (S ⊢ τ2 ⊑ τ3 ⇒ (∀ τ1. τ1 ⊑ τ2 ⇒ S ⊢ τ1 ⊑ τ3))
apply (induct rule: consistent-equal-consistent-less.induct) by auto
lemma consless-trans: [ τ1 ⊑ τ2; S ⊢ τ2 ⊑ τ3 ] ⇒ S ⊢ τ1 ⊑ τ3
using consless-trans-impl by blast
lemma **conseq-refl**: $S \vdash \tau \simeq \tau$
apply (induct $\tau$) apply blast+ done

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

lemma **conseq-symm**: $S \vdash \tau \simeq \tau' \Rightarrow S \vdash \tau' \simeq \tau$
using conseq-symm-impl by blast

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

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

lemma **less-no-dyn-equal**: $[ [ S \vdash \tau \sqsubseteq \tau'; \text{no-dyn } \tau ] ] = S \tau = \tau'$
using conseq-less-no-dyn-equal-impl by blast

lemma **less-conseq-less-impl**: $(S \vdash \tau_1 \simeq \tau_2 \rightarrow \text{True})$
$\land (S \vdash \tau \subseteq \tau'' \rightarrow \text{no-dyn } \tau \rightarrow (\forall \tau', \text{no-dyn } \tau' \land S \vdash \tau \simeq \tau' \rightarrow S \vdash \tau' \subseteq \tau''))$
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 simp apply simp apply simp apply simp apply (rule implI) apply simp
apply (case_tac no-dyn $\sigma$) apply simp
apply clarify
apply (erule conseq-fun-any)
apply simp apply simp
apply (case_tac no-dyn $\tau''$) apply simp
prefer 2 apply simp
apply (rule CLFun)
apply force
apply force
apply simp
apply (rule CLVar)
apply (erule consless-fun-any)
apply simp
apply (rule conjI)
proof
  fix $S \sigma \sigma' \tau \tau' \tau'a \alpha \tau'' \tau'b$
  assume st: $S \vdash \sigma \sqsubseteq \tau$ and ns: no-dyn $\sigma$ and stt: $S \vdash \sigma \sqsubseteq \tau''$
  from st ns have sst: $S \sigma = \tau$ by (rule less-no-dyn-equal)
  from stt ns have $S \sigma = \tau''$ by (rule less-no-dyn-equal)
with sst show $\tau'' = \tau$ by simp

next

fix $S \sigma \sigma' \tau \tau' \alpha \tau'' \tau'b$

assume st: $S \vdash \sigma' \subseteq \tau'$ and ns: no-dyn $\sigma'$ and sst: $S \vdash \sigma' \subseteq \tau'b$

from st ns have sst: $S \sigma' = \tau'$ by (rule less-no-dyn-equal)

from stt ns have $S \sigma' = \tau'b$ by (rule less-no-dyn-equal)

with sst show $\tau'b = \tau'$ by simp

qed

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

$\Rightarrow S \vdash \tau' \subseteq \tau''$

using less-conseq-less-impl by blast

lemma less-less-conseq-impl:

(S \vdash \tau \simeq \tau' \longrightarrow True ) \land

(S \vdash \tau \subseteq g \longrightarrow ( \forall \tau'. S \vdash \tau' \subseteq g \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 clarify apply (rule consless-any-fun) apply auto

done

lemma less-less-conseq:

$[ S \vdash \tau \subseteq g ; S \vdash \tau' \subseteq g ] \Longrightarrow S \vdash \tau \simeq \tau'$

using less-less-conseq-impl by blast

lemma subst-typeof: $S \ (\text{OfType } c) = \text{OfType } c$

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 \tau \sim S \tau' ) \land (S \vdash \tau \subseteq \tau' \longrightarrow 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 using less-info-implies-consistent apply blast

apply simp

apply (frule less-info-implies-consistent)

apply (frule consistent-symmetric) apply simp

apply force+

done

lemma cons-eq-implies-cons:
\[ S \vdash \tau \simeq \tau' \implies SS \tau \sim SS \tau' \]

**Using ce-less-implies-cons-less by blast**

**Lemma** cons-less-implies-less:
\[ S \vdash \tau \sqsubseteq \tau' \implies SS \tau \sqsubseteq SS \tau' \]

**Using ce-less-implies-cons-less by blast**

**Lemma** conseq-any-fun-var:
\[ S \vdash \tau \simeq \tau' \mapsto UVarT \beta \implies \tau = ? \lor (\exists t \ t_1 \ t_2. SS \tau = t_1 \rightarrow t_2 \land t_1 \sim SS \tau' \land t_2 \sqsubseteq \%S \beta) \]

**Apply** (case-tac \( \tau \))

**Defer**

**Apply** force

**Apply** force

**Apply** simp

**Apply** (erule conseq-fun-fun) apply (rule conjI)

**Apply** (rule cons-eq-implies-cons) apply simp

**Apply** (erule conseq-any-uar)

**Apply** simp apply force

**Apply** (rule cons-less-implies-less) apply simp

**Apply** simp apply (erule consless-uar-any) apply force

**Proof** –

**Fix** \( \alpha \) assume \( ttb : S \vdash \tau \simeq \tau' \mapsto UVarT \beta \) and \( t : \tau = UVarT \alpha \)

**From** \( ttb \ t \) have \( tba : S \vdash \tau' \mapsto UVarT \beta \sqsubseteq \%S \alpha \)

**Apply** simp apply (erule conseq-uar-fun) by blast

**From** \( tba \) obtain \( t_1 \ t_2 \) where \( t_{t_1} : S \vdash \tau' \sqsubseteq t_1 \) and \( b_{t_2} : S \vdash UVarT \beta \sqsubseteq t_2 \)

**And** \( sa : \%S \alpha = t_1 \rightarrow t_2 \) using conseq-fun-var-aur by blast

**From** \( t_{t_1} \) have \( SS \tau' \sqsubseteq t_1 \) by (rule cons-less-implies-less)

**Hence** \( t_{t_1} : t_1 \sim SS \tau' \) using less-info-implies-consistent consistent-symmetric by blast

**From** \( b_{t_2} \) have \( \%S \beta = t_2 \) by force

**Hence** \( t_{t_2 b} : t_2 \sqsubseteq \%S \beta \) by force

**From** \( t \ sa \ t_{t_1} \ t_{t_2 b} \)

**Show** \( \tau = ? \lor (\exists t \ t_1 \ t_2. SS \tau = t_1 \rightarrow t_2 \land t_1 \sim SS \tau' \land t_2 \sqsubseteq \%S \beta) \) by simp

**Qed**

**Lemma** conseq-any-fun-rule:
\[ \[ \begin{array}{c} S \vdash \tau \simeq \tau' \mapsto UVarT \beta; \\
\tau = ? \implies P; \\
\land \ t_1 \ t_2. [ SS \tau = t_1 \rightarrow t_2 ; t_1 \sim SS \tau' ; t_2 \sqsubseteq \%S \beta ] \implies P \\
\end{array} \] \]

**Apply** (erule conseq-any-fun-var) apply (erule disjE)

**Apply** simp

**Apply** (erule ezE)+ apply simp apply clarify

**Apply** (case-tac \( SS \tau \)) apply force apply force apply force apply force apply force apply force apply force

**Apply** simp apply clarify apply simp

**Proof** –

**Fix** \( t \ t_1 \ t_2 \)

**Assume** \( A : \land t_{t_1} t_{t_2}. [ t_{t_1} = t_{t_1} \land t_2 = t_{t_2}; t_{t_1} \sim SS \tau' ; t_{t_2} \sqsubseteq \%S \beta ] \implies P \)

**And** \( B : t_1 \sim SS \tau' \) and \( C : t_2 \sqsubseteq \%S \beta \)

**From** \( A[of \ t_{t_1} \ t_{t_2}] \ B \ C \) show \( P \) apply blast done

**Qed**

**Lemma** prop1-item-6-and-7-fwd:
\[ (S \vdash t_1 \sim t_2 \rightarrow FTV t_1 = \{} \land FTV t_2 = \{} \rightarrow t_1 \sim t_2) \]
\[ (S \vdash t_1 \subseteq t_2 \implies \text{FTV } t_1 = \{ \} \rightarrow t_1 \subseteq t_2) \]

apply (induct rule: consistent-equal-consistent-less.induct)
apply blast apply blast apply blast apply blast
apply clarify apply simp apply (rule CFun) apply simp apply simp
apply simp apply simp apply simp apply blast apply blast apply blast
apply clarify apply (rule LEFun) apply simp apply simp
apply blast apply blast done

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

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

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

lemma widen-conseq-consless:
\[ (S \vdash t_1 \sim t_2 \implies (\forall \alpha. \alpha \in \text{FTV } \tau_1 \cup \text{FTV } \tau_2 \rightarrow \%S' \alpha = \%S \alpha) \]
\[ \rightarrow S' \vdash t_1 \sim t_2) \]
\[ \land (S \vdash t_1 \subseteq t_2 \implies (\forall \alpha. \alpha \in \text{FTV } \tau_1 \rightarrow \%S' \alpha = \%S \alpha) \]
\[ \rightarrow S' \vdash t_1 \subseteq t_2) \]
apply (induct rule: consistent-equal-consistent-less.induct)
apply force+ done

lemma widen-conseq:
\[ S \vdash t_1 \sim t_2; (\forall \alpha. \alpha \in \text{FTV } \tau_1 \cup \text{FTV } \tau_2 \rightarrow \%S' \alpha = \%S \alpha) \]
\[ \implies S' \vdash t_1 \sim t_2 \]
using widen-conseq-consless by blast

lemma widen-consless:
\[ S \vdash t_1 \subseteq t_2; (\forall \alpha. \alpha \in \text{FTV } \tau_1 \rightarrow \%S' \alpha = \%S \alpha) \]
\[ \implies S' \vdash t_1 \subseteq t_2 \]
using widen-conseq-consless by blast

A.7 The Gradual Type System with Type Variables

inductive igtlc-wt :: [subt, eun, nat, nat] \Rightarrow [expr,ty] \Rightarrow bool (-:::- \vdash_g - :: [52,52,52,52,52,52] 51)
where
GVar[intro]: [lookup \Gamma x = \text{Some } \tau ] \implies S;\Gamma;n;\vdash_g \text{Var } x : \tau |
GConst[intro]: S;\Gamma;n;\vdash_g \text{Const } c : \text{TypeOf } c |
GAbs[intro]: S;(x,\tau_1)\#\Gamma;m;\vdash_g e : \tau_2 ] \implies S;\Gamma;m;\vdash_g (\lambda x:\tau_1. e) : \tau_1 \rightarrow \tau_2 |
lemma ftv-env-ftv-ty [rule-format]:
\[ \forall x \sigma. \text{lookup } \Gamma \ x = \text{Some } \tau \to FTV \ \tau \subseteq FTV \ \Gamma \]
apply (induct \( \Gamma \)) by auto

lemma igtlc-fresh-grows:
\[ S; \Gamma ; m n \vdash e : \tau \to m \leq n \]
apply (induct rule: igtlc-ut.induct)
apply simp+ done

lemma igtlc-ftv-result:
\[ S; \Gamma ; m n \vdash e : \tau \to (\forall \alpha. \alpha \in FTV \ \tau \to \alpha \in FTV \ \Gamma \cup FTV \ e \vee (m \leq \alpha \land \alpha < n)) \]
(is \[ S; \Gamma ; m n \vdash e : \tau \to \exists \mathcal{P} \ S \ \Gamma \ m n e \tau \]
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 \( S \) \( \tau_1 \) \( \tau_2 \) \( m \) \( n \) \( x \)
assume \[ S; (x; \tau_1) \# \Gamma ; m n \vdash e : \tau_2 \]
and IH: \( \forall \alpha. \alpha \in FTV \ \tau_2 \to \alpha \in FTV \ ((x; \tau_1) \# \Gamma) \cup FTV \ e \vee m \leq \alpha \land \alpha < n \)
show \( \exists \mathcal{P} \ S \ \Gamma \ m n \ (\lambda \alpha \tau_1. \ e) (\tau_1 \to \tau_2) \)
apply (rule allI) apply (rule impI)

proof –
fix \( \alpha \)
assume af12: \( \alpha \in FTV \ (\tau_1 \to \tau_2) \)
from af12 have \( \alpha \in FTV \ \tau_1 \lor \alpha \in FTV \ \tau_2 \) by simp
moreover \{ assume af1: \( \alpha \in FTV \ \tau_1 \)
from af1 have \( \alpha \in FTV \ (\lambda x \tau_1. \ e) \) by simp
hence \( \alpha \in FTV \ \Gamma \cup FTV \ (\lambda x \tau_1. \ e) \vee m \leq \alpha \land \alpha < n \) by simp
\}
moreover \{ assume af2: \( \alpha \in FTV \ \tau_2 \)
from af2 IH have \( \alpha \in FTV \ ((x; \tau_1) \# \Gamma) \cup FTV \ e \vee m \leq \alpha \land \alpha < n \) by simp
moreover \{ assume \( \alpha \in FTV \ ((x; \tau_1) \# \Gamma) \)
\]
moreover \{ assume \( \alpha \in FTV \ (\lambda x \tau_1. \ e) \) by simp
moreover \{ assume \( \alpha \in FTV \ (\lambda x \tau_1. \ e) \vee m \leq \alpha \land \alpha < n \) by simp
\}
moreover \{ assume \( m \leq \alpha \land \alpha < n \)
moreover \{ assume \( \alpha \in FTV \ \Gamma \cup FTV \ (\lambda x \tau_1. \ e) \vee m \leq \alpha \land \alpha < n \) by simp
\}
ultimately have \( \alpha \in FTV \ \Gamma \cup FTV \ (\lambda x \tau_1. \ e) \vee m \leq \alpha \land \alpha < n \) by blast
ultimately show \( \alpha \in FTV \ \Gamma \cup FTV \ (\lambda x \tau_1. \ e) \vee m \leq \alpha \land \alpha < n \) by blast
qed

next
fix \( S \) \( \tau_1 \) \( \tau_2 \) \( e \) \( e' \) \( n_0 \) \( n_1 \) \( n_2 \)
assume wte: \[ S; \Gamma ; n_0 n_1 \vdash e : \tau_1 \]
and IH1: \( \forall \alpha. \alpha \in FTV \ \tau_1 \to \alpha \in FTV \ \Gamma \cup FTV \ e \vee n_0 \leq \alpha \land \alpha < n_1 \)
and wtep: \[ S; \Gamma ; n_1 n_2 \vdash e' : \tau_2 \]
and IH2: \( \forall \alpha. \alpha \in FTV \ \tau_2 \to \alpha \in FTV \ \Gamma \cup FTV \ e' \vee n_1 \leq \alpha \land \alpha < n_2 \)
and s12b: \( S \vdash \tau_1 \simeq \tau_2 \to UVarT \ n_2 \)
show \( \forall \alpha. \alpha \in FTV \ (UVarT \ n_2) \to \alpha \in FTV \ \Gamma \cup FTV \ (App \ e \ e') \vee n_0 \leq \alpha \land \alpha < Suc \ n_2 \)
apply (rule allI) apply (rule impI)

proof –
fix \( \alpha \)
assume \( \alpha \in FTV \ (UVarT \ n_2) \) hence an2: \( \alpha = n_2 \) by simp
from \(an2\) have \(\alpha < Suc \ n2\) by simp
from \(wte\) have \(n0n1\): \(n0 \leq n1\) by (rule \(igtlc\)-fresh-grows)
from \(wtep\) have \(nIn2\): \(n1 \leq n2\) by (rule \(igtlc\)-fresh-grows)
from \(n0n1 \ nIn2 \ an2\) have \(n0a\): \(n0 \leq \alpha\) by simp
from \(n0a \ an2\) show \(\alpha < Suc \ n2\) by simp
qed

lemma widen-subst-impl:
\[
\begin{align*}
S; \Gamma; m; n \vdash_g e & : \tau \\
(\forall \alpha. \alpha \in FTV \ (\forall x. x) \# \Gamma) \cup FTV e \lor \tau & \longrightarrow \%S' \alpha = \%S \alpha \\
\longrightarrow S'; \Gamma; m; n \vdash_g e & : \tau \\
(is \ S; \Gamma; m; n \vdash_g e & : \tau \longrightarrow \%P \ S \ \Gamma \ m \ n \ e \ \tau)
\end{align*}
\]
apply (induct rule: \(igtlc\)-art.induct)
apply force
apply force

proof
fix \(S \ \Gamma \ \tau1 \ \tau2 \ \ m \ n \ x\)
assume \(S; \Gamma; (x, \tau1) \# \Gamma; m; n \vdash_g e : \tau2\)
and \(IH:\ (\forall \alpha. \alpha \in FTV \ ((x, \tau1) \# \Gamma) \cup FTV e \lor \tau) \longrightarrow \%S' \alpha = \%S \alpha\)
with \(\alpha < Suc \ n2\)
show \(\forall \alpha. \alpha \in FTV \ (\forall x. x) \# \Gamma) \cup FTV e \lor \tau) \longrightarrow \%S' \alpha = \%S \alpha\)
proof clarify
assume \(\beta:\ (\forall \alpha. \alpha \in FTV \ (\forall x. x) \# \Gamma) \cup FTV e \lor \tau) \longrightarrow \%S' \alpha = \%S \alpha\)
from \(\beta\) have \(\forall \alpha. \alpha \in FTV \ ((x, \tau1) \# \Gamma) \cup FTV e \lor \tau) \longrightarrow \%S' \alpha = \%S \alpha\)
apply clarify apply (erule disjE)
apply simp apply (erule disjE)
apply (erule-tac \(x=\alpha\) in allE) apply (simp add: \(FTV\)-pair)
apply blast
apply blast
done

with \(IH\) show \(S'; (x, \tau1) \# \Gamma; m; n \vdash_g e : \tau2\) by simp
qed

next
fix \(S \ \Gamma \ \tau1 \ \tau2 \ \ e' \ \ n0 \ n1 \ n2\)
assume \(wte\): \(S; \Gamma; n0; n1 \vdash_g e : \tau1\)
and \(wtep:\ S; \Gamma; n1; n2 \vdash_g e' : \tau2\)
and \(IH1:\ \%P \ S \ \Gamma \ n0 \ n1 \ e \ \tau1\)
and \(IH2:\ \%P \ S \ \Gamma \ n1 \ n2 \ e' \ \tau2\)
and \(st12b:\ S \vdash \tau1 \simeq \tau2 \longrightarrow UVarT \ n2\)
show \(\%P \ S \ \Gamma \ n0 \ (Suc \ n2) \ (App \ e \ e') \ (UVarT \ n2)\)
proof clarify
assume \(fa:\ (\forall \alpha. \alpha \in FTV \ (\forall x. x) \# \Gamma) \cup FTV e \lor \tau) \longrightarrow \%S' \alpha = \%S \alpha\)
from \(wte\) have \(n0n1\): \(n0 \leq n1\) by (rule \(igtlc\)-fresh-grows)
from \(wtep\) have \(n1n2\): \(n1 \leq n2\) by (rule \(igtlc\)-fresh-grows)
from \(fa \ nIn2\)
have \(fe:\ (\forall \alpha. \alpha \in FTV \ (\forall x. x) \# \Gamma) \cup FTV e \lor \tau) \longrightarrow \%S' \alpha = \%S \alpha\)
by simp
from \(fe \ IH1\) have \(wte2:\ S; \Gamma; n0; n1 \vdash_g e : \tau1\) by simp
from \(fa \ n0n1\)
have \(fep:\ (\forall \alpha. \alpha \in FTV \ (\forall x. x) \# \Gamma) \cup FTV e \lor \tau) \longrightarrow \%S' \alpha = \%S \alpha\)
by simp
from \(fep \ IH2\) have \(wtep2:\ S; \Gamma; n1; n2 \vdash_g e' : \tau2\) by simp
from \(wte2 \ fe\) have \(af1:\ (\forall \alpha. \alpha \in FTV \ \tau1 \longrightarrow \%S' \alpha = \%S \alpha)\)
using \(igtlc\)-fv-result apply blast done
from wtep2 fep have af2: \((\forall \alpha. \alpha \in FTV \tau_2 \rightarrow %S' \alpha = %S \alpha)\)
  using igtlc-ftv-result apply blast done
from wte have n̸n1: n̸0 \leq n̸1 by (rule igtlc-fresh-grows)
from wtep have n̸n2: n̸1 \leq n̸2 by (rule igtlc-fresh-grows)
from fa n̸n1 n̸n2 have \((\forall \alpha. \alpha \in FTV (UVarT n̸2) \rightarrow %S' \alpha = %S \alpha)\) by auto
with af1 af2 have af12b: \((\forall \alpha. \alpha \in FTV \tau_1 \cup FTV (\tau_2 \rightarrow UVarT n̸2) \rightarrow %S' \alpha = %S \alpha)\) by simp
from st12b af12b have S' \vdash \tau_1 \simeq \tau_2 \rightarrow UVarT n̸2 by (rule widen-conseq)
with wte2 wtep2 show S';\Gamma;\tau_0;Succ n̸2 \vdash_g \text{App } e' : UVarT n̸2 by blast
qed

lemma widen-subst:
\[
\begin{array}{ll}
S;\Gamma;m;n \vdash_g e : \tau; (\forall \alpha. \alpha \in FTV \Gamma \cup FTV e \cup (m \leq \alpha \wedge \alpha < n) \rightarrow %S' \alpha = %S \alpha) & \rightarrow S';\Gamma;\tau_0;Succ n̸2 \vdash_g \text{App } e' : UVarT n̸2 by blast
\end{array}
\]

— Theorem 2

theorem igtlc-implies-glnc:
\[
\begin{array}{ll}
S;\Gamma;m;n \vdash_g e : \tau \Rightarrow FTV \Gamma = \{\} \wedge FTV e = \{\} & \rightarrow \{\exists \tau'. \Gamma \vdash_g e : \tau' \wedge \tau' \subseteq %S \tau\}
\end{array}
\]
(is S;\Gamma;m;n \vdash_g e : \tau \Rightarrow ?P S \Gamma e \tau)

proof (induct rule: igtlc-wt.induct)
fix \Gamma:env and \tau and x and S n assume gx: lookup \Gamma x = Some \tau
show ?P S \Gamma (Var x) \tau
proof clarify
  assume fg: FTV \Gamma = \{\}
  from gx fg have FTV \tau = \{\} using ftw-env-ftw-tg by blast
  hence \(\forall a. a \in FTV \tau \rightarrow %S a = UVarT a\) by simp
  hence %S \tau = \tau using ftv-dom-id by blast
  hence \tau \subseteq %S \tau apply simp by (rule less-info-refl)
  with gx show \exists \tau'. \Gamma \vdash_g \text{Var } x : \tau' \wedge \tau' \subseteq %S \tau by blast
qed

next
fix S \Gamma c show ?P S \Gamma (Const c) (TypeOf c) by auto
next
fix S:subst and x \tau_1 and \Gamma::env and m n e \tau_2
assume IH: ?P S ((x,\tau_1)#\Gamma) e \tau_2
show ?P S \Gamma (\lambda x:\tau_1. e) (\tau_1 \rightarrow \tau_2)
proof clarify
  assume fg: FTV \Gamma = \{\} and ft: FTV (\lambda x:\tau_1. e) = \{\}
  from ft have ft': FTV \tau_1 = \{\} by simp
  with fg have fg2: FTV ((x,\tau_1)#\Gamma) = \{\} by (simp add: FTV-fun)
  from ft have fe: FTV e = \{\} by simp
  from fg2 fe IH obtain \tau' where wte: (x,\tau_1)#\Gamma \vdash_g e : \tau'
    and tsp12: \tau' \subseteq %S \tau_2 by blast
  from ft have \(\forall a. a \in FTV \tau_1 \rightarrow %S a = UVarT a\) by simp
  hence %S \tau_1 = \tau_1 using ftv-dom-id by blast
  with tsp22 have stt: \tau_1 \rightarrow \tau' \subseteq %S (\tau_1 \rightarrow \tau_2)
    apply simp apply (rule LEFun) apply (rule less-info-refl) apply simp done
from wte have \Gamma \vdash_g \lambda x:\tau_1. e : \tau_1 \rightarrow \tau' by blast
with stt show \exists \tau'. \Gamma \vdash_g \lambda x:\tau_1. e : \tau' \wedge \tau' \subseteq %S (\tau_1 \rightarrow \tau_2)
  apply (rule_tac x=\tau_1 \rightarrow \tau' 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: $S \vdash \tau_1 \simeq \tau_2 \rightarrow UVarT n2$
show $?P S \Gamma (App e e') (UVarT n2)$
proof clarify
assume fg: $FTV \Gamma = \{\}$
and fa: $FTV (App e e') = \{\}$
from fa have fc: $FTV e = \{\}$ by simp
with fg IH1 obtain t1 where wte: $\Gamma \vDash_g e : t1$
and t11: $t1 \subseteq \{\} S \tau_1$ by blast
from fa have fep: $FTV e' = \{\}$ by simp
with fg IH2 obtain t2 where wtep: $\Gamma \vdash_g e' : t2$
and st2: $t2 \subseteq \{\} S \tau_2$ by blast
from st12b show $\exists \tau' . \Gamma \vdash_g App e e' : \tau' \land \tau' \subseteq \{\} S (UVarT n2)$
proof (rule conseq-any-fun-var-rule)
assume t1d: $\tau_1 = \?$
with t11 have T1d: $t1 = \? \Gamma$ by auto
from wte T1d have wte2: $\Gamma \vdash_g e : \? \Gamma$ by simp
with wtep have $A : \Gamma \vdash_g App e e' : \? \Gamma$ by blast
have $B : \? \subseteq \{\} S (UVarT n2)$ by blast
from A B show ?thesis by blast
next
fix t11 t12 assume st1: $S \tau_1 = t11 \rightarrow t12$ and st1t2: $t11 \sim \{\} S \tau_2$
and st2: $t12 \subseteq \{\} S n2$
from t11 st1 have t1-le-t12: $t1 \subseteq t11 \rightarrow t12$ by simp
from t11t2 st2 have $\tau_2 \sim t11$ by (rule consistent-symmetric)
from t1-le-t12 show ?thesis
proof (rule le-any-fun)
fix $\sigma \sigma' \Gamma \vdash_g e : \sigma \rightarrow \sigma'$
and T1: $t1 = \sigma \rightarrow \sigma'$
with wte have wte2: $\Gamma \vdash_g e : \sigma \rightarrow \sigma'$ by simp
from st2 st2t11 have t2t11: $t2 \sim t11$ by (rule less-cons-implies-cons)
from t1t12: $t11 \sim t2$ by (rule consistent-symmetric)
from st11 t11t2 have $\sigma \sim t2$ by (rule less-cons-implies-cons)
from t12: $t2 \sim \sigma$ by (rule consistent-symmetric)
from wte2 have wtep t2s have $A : \Gamma \vdash_g App e e' : \sigma' \Gamma$ by blast
from wtep t2s have $\sigma' \subseteq \{\} S n2$ by (rule less-info-transitive)
from A B have $\sigma' \subseteq \{\} S (UVarT n2)$ by simp
from A B show $\exists \tau' . \Gamma \vdash_g App e e' : \tau' \land \tau' \subseteq \{\} S (UVarT n2)$ by blast
next
assume T1d: $t1 = \?$
from wte T1d have wte2: $\Gamma \vdash_g e : \? \Gamma$ by simp
with wtep have $A : \Gamma \vdash_g App e e' : \? \Gamma$ by blast
have $B : \? \subseteq \{\} S (UVarT n2)$ by blast
from A B have ?thesis by blast
qed
qed
qed

lemma lookup-subst-subst:
lookup $\Gamma x = \text{Some } \tau \Longrightarrow$ lookup ($\{\} S \Gamma x = \text{Some } (\{\} S \tau)$
apply (induct $\Gamma$)
apply simp

42
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

**theorem igtlc-wt-implies-glcl:**

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

**proof (induct rule: igtlc-wt_induct):**

fix \( \Gamma : env \) and \( \exists \ x \ S \ n \) assume lookup \( \Gamma \) \( x = Some \ \tau \)
thus \( \exists \ \tau'. \ S \ \Gamma \vdash g \ S (Var \ x) : \tau' \land \exists \ S \tau \)
apply simp apply (rule_tac x=\$S \tau \ in \ exI) apply (rule conjI)
apply (rule WTVar) apply (simp add: lookup-subst-subst) apply blast done

next

fix \( S \ \Gamma \ n \ c \) show \( \exists \ \tau'. \ S \ \Gamma \vdash g \ S (Const \ c) : \tau' \land \exists \ S (TypeOf \ c) \)
apply simp apply blast done

next

fix \( S \ x \ \tau_1 \ \Gamma \ m \ n \ e \ \tau_2 \)
assume \( \text{IH1}: \exists \ \tau'. \ S \ ((x,\tau_1)\#\Gamma) \vdash g \ S e : \tau' \land \exists \ S \tau_2 \)
from \( \text{IH} \) obtain \( \tau' \) where \( \text{wte}: \exists \ S ((x,\tau_1)\#\Gamma) \vdash g \ S e : \tau' \)
and \( \text{tst}: \tau' \subseteq \exists \ S \tau_2 \) by blast
from \( \text{wte} \) have \( (x,S\tau_1)\#(S \ \Gamma) \vdash g \ S e : \tau' \) by (simp only: subst-extend-env)

next

fix \( S \ \Gamma \ n_0 \ n_1 \ e \ \tau_1 \ n_2 \ e' \ \tau_2 \)
assume \( \text{IH1}: \exists \ \tau'. \ S \ \Gamma \vdash g \ S e : \tau' \land \exists \ S \tau_1 \)
and \( \text{IH2}: \exists \ \tau'. \ S \ \Gamma \vdash g \ S e' : \tau' \land \exists \ S \tau_2 \)
and \( t12\vdash: \exists \ \tau_1 \vdash \exists \ \tau_2 \implies \UVarT \ n_2 \)
from \( \text{IH1} \) obtain \( t1' \) where \( \text{wte}: \exists \ S \ \Gamma \vdash g \ S e : \tau1' \)
and \( \text{tst}: \exists \ t1' \subseteq \exists \ S \tau_1 \) by blast
from \( \text{IH2} \) obtain \( t2' \) where \( \text{wtep}: \exists \ S \ \Gamma \vdash g \ S e' : \tau2' \)
and \( \text{tpst}: \exists \ t2' \subseteq \exists \ S \tau_2 \) by blast
from \( t12\vdash \) show \( \exists \ \tau': \exists \ S \ \Gamma \vdash g \ S \ (App \ e \ e') : \tau' \land \exists \ S (\UVarT \ n_2) \)

**proof (rule conseq-ang-fun-var-rule):**

assume \( \text{t1}: \exists \ \tau_1 = ? \)
from \( t1 \) \( t1\vdash \) have \( \text{t1p}: \exists \ t1' = ? \) by auto
with \( \text{wte} \) have \( \text{wte}: \exists \ S \ \Gamma \vdash g \ S e : ? \) by simp
from \( \text{wte} \) \( \text{wtep} \) have \( \exists \ S \ \Gamma \vdash g \ S \ (App \ e \ e') : ? \) by (rule \ WTApp1)
thus \( \exists \ \tau': \exists \ S \ \Gamma \vdash g \ S \ (App \ e \ e') : \tau' \land \exists \ S (\UVarT \ n_2) \) apply simp by blast

next

fix \( t1 \) \( t2 \)
assume \( \text{st1}: \exists \ S \ \tau_1 \vdash \exists \ \tau_2 \) and \( \text{st2}: \exists \ S \ \tau_1 \vdash \exists \ S \tau_2 \)
from \( t1\vdash \) \( t1\vdash \) have \( \text{t1p12}: \exists \ t1' \subseteq \exists \ t1 \implies \exists \ t2 \) by simp

moreover \{ assume \( \text{t1p}: \exists \ t1' = ? \)
with \( \text{wte} \) have \( \text{wte}: \exists \ S \ \Gamma \vdash g \ S e : ? \) by simp
from \( \text{wte} \) \( \text{wtep} \) have \( \exists \ S \ \Gamma \vdash g \ S \ (App \ e \ e') : ? \) by (rule \ WTApp1)

moreover \{ assume \ X: \exists \ t11 \ t12. \ t1' = t11 \implies t12 \)
from \( X \) obtain \( t11 \ t12 \) where \( \text{T1}: \exists \ t1' \vdash \exists \ t12 \) by blast
from \( \text{T1} \) \( t1p12 \) have \( \text{t11t1}: \exists \ t1 \vdash \exists \ t1 \) by blast

43
from \( T1 \) \( \text{t1p12} \) have \( \text{t12t2} \): \( \text{t12} \subseteq \text{t2} \) by blast
from \( \text{wte} \) \( \text{T1} \) have \( \text{wte2} : \$ \text{S} \Gamma_\text{g} \$ \text{S} \text{e} : \text{t11} \rightarrow \text{t12} \) by simp
from \( \text{t11t1} \) \( \text{t1s} \) have \( \text{t11st2} : \text{t11} \sim \$\$ \text{S} \tau_2 \) by (rule less-cons-implies-cons)

hence \( \text{st2t11} : \$ \text{S} \tau_2 \sim \text{t11} \) by (rule consistent-symmetric)

from \( \text{tpst2} \) \( \text{st2t11} \) have \( \text{t2t11} : \text{t2} \sim \text{t11} \) by (rule less-cons-implies-cons)

from \( \text{wte2} \) \( \text{wtp} \) \( \text{t2t11} \) have \( \text{wta} : \$\$ \text{S} \Gamma_\text{g} \) \( \text{App} \) \( \$\$ \text{S} \text{e} \) \( \$\$ \text{S} \text{e}' \) : \( \text{t12} \)

by (rule WTApp2)

from \( \text{t12t2} \) \( \text{t2b} \) have \( \text{t12b} : \text{t12} \subseteq \% \text{S} \text{n2} \) by (rule less-info-transitive)

from \( \text{wta} \) \( \text{t12b} \) have \( \exists \text{'} \). \$ \text{S} \Gamma_\text{g} \$ \text{S} \) \( \text{App} \) \( \$\$ \text{S} \text{e} \) \( \$\$ \text{S} \text{e}' \) : \( \text{t2} \)

apply simp by blast

} ultimately show \( \exists \text{'} \). \$ \text{S} \Gamma_\text{g} \$ \text{S} \) \( \text{App} \) \( \$\$ \text{S} \text{e} \) \( \$\$ \text{S} \text{e}' \) : \( \text{t2} \)

by blast

qed

qed

— This is Theorem 4 of the paper

**Theorem igtlc-wt-no-dyn-implies-istlc:**

\( S; \Gamma ; m:n \vdash_g e : \tau \Rightarrow \text{no-dyn} \) \( \Gamma \wedge \text{no-dyn} \) \( e \rightarrow S; \Gamma \vdash e : \tau \wedge \text{no-dyn} \) \( \tau \)

apply (induct rule: igtlc-wt.induct)

apply clarify apply (rule conjI) apply force

apply (induct: add: no-dyn-lookup)

apply clarify apply (rule conjI) apply force

apply (induct: 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 (case-tac no-dyn \( \tau_1 \))

apply simp apply simp

apply clarify

proof —

fix \( S \) \( \Gamma \) \( n_0 \) \( n_1 \) \( e_1 \) \( \tau_1 \) \( n_2 \) \( e_1' \) \( \tau_2 \)

assume \( \text{st12b} \): \( S \vdash \tau_1 \sim \tau_2 \rightarrow \text{UVarT} \) \( n_2 \) and \( \text{ndg} : \text{no-dyn} \) \( \Gamma \)

and \( \text{nfa} : \text{no-dyn} \) \( \text{App} \) \( e e' \)

and \( \text{IH1} : \text{no-dyn} \) \( \Gamma \wedge \text{no-dyn} \) \( e \rightarrow S; \Gamma \vdash e : \tau_1 \wedge \text{no-dyn} \) \( \tau_1 \)

and \( \text{IH2} : \text{no-dyn} \) \( \Gamma \wedge \text{no-dyn} \) \( e' \rightarrow S; \Gamma \vdash e' : \tau_2 \wedge \text{no-dyn} \) \( \tau_2 \)

from \( \text{ndg} \) \( \text{nda} \) \( \text{IH1} \) have \( \text{wte} : S; \Gamma \vdash e : \tau_1 \) by auto

from \( \text{ndg} \) \( \text{nda} \) \( \text{IH1} \) have \( \text{ndt1} : \text{no-dyn} \) \( \tau_1 \) by auto

from \( \text{ndg} \) \( \text{nda} \) \( \text{IH2} \) have \( \text{wtep} : S; \Gamma \vdash e' : \tau_2 \) apply auto apply (case-tac no-dyn \( e \))

apply simp apply simp done

from \( \text{ndg} \) \( \text{nda} \) \( \text{IH2} \) have \( \text{ndt2} : \text{no-dyn} \) \( \tau_2 \) apply auto apply (case-tac no-dyn \( e \))

apply simp apply simp done

from \( \text{ndt2} \) have \( \text{ndt2b} : \text{no-dyn} \) \( \tau_2 \rightarrow \text{UVarT} \) \( n_2 \) by simp
\begin{verbatim}
from st12b ndt1 ndt2b have st1t2b: \$S \tau_1 = \$S (\tau_2 \rightarrow UVarT n2)
   by (rule consq-no-dyn-equal)
from wte wtep st1t2b show \$T \Gamma \vdash App e e' : UVarT n2 \land no-dyn (UVarT n2)
   by force
qed
\end{verbatim}

References


