Formal Proof of Type Preservation of the Dictionary Passing Transform for System F

Marius Weidner

Chair of Programming Languages, University of Freiburg
`weidner@cs.uni-freiburg.de`

Bachelor Thesis

Examiner: Prof. Dr. Peter Thiemann
Advisor: Hannes Saffrich

Abstract. Most popular strongly typed programming languages support function overloading. In combination with polymorphism this leads to essential language constructs, for example typeclasses in Haskell or traits in Rust. We introduce System F_O, a minimal language extension to System F, with support for overloading. Furthermore, we prove the Dictionary Passing Transform from System F_O to System F to be type preserving using Agda.

Table of Contents

1 Introduction

1.1 Overloading in Programming Languages

Overloading function names is a practical technique to overcome verbosity in real world programming languages. In every language there exist commonly used function names and operators that are defined for a variety of type combinations. Overloading the meaning of function names for different type combinations helps overcome this verbosity. Overloading is sometimes also referred to as ad-hoc polymorphism. Python, for example, uses magic methods to overload commonly used operators on user defined classes and Java utilizes method overloading. Both Python and Java implement rather restricted forms of overloading. Haskell solves the overloading problem with a more general concept, called typeclasses.

1.2 Typeclasses in Haskell

Essentially, typeclasses allow to declare function names with generic type signatures. We can give one of possibly many meanings to a typeclass by instantiating the typeclass for concrete types. Instantiating a typeclass gives an actual implementation to all functions defined by the typeclass based on the concrete types that the typeclass is instantiated for. When we invoke an overloaded function name defined by a typeclass, we expect the compiler to determine the correct instance based on the types of the arguments that were applied to the overloaded function name. Furthermore, Haskell allows to constrain a type variable α via type constraints $\mathtt{Tc}\ \alpha \Rightarrow \tau'$ to only be substituted by a concrete type τ if there exists an instance $\mathtt{Tc}\ \tau$. Type constraints allow to abstract over all types that inherit a specific behavior that can differ for each types that implements the behavior. Thus type constraints are a powerful formalism in addition to normal parametric polymorphism.

Example: Overloading Equality in Haskell

In this example the function $\mathtt{eq} : \alpha \to \alpha \to \mathtt{Bool}$ is overloaded with different meanings for different substitutions $\{\alpha \mapsto \tau\}$. We want to be able to call eq on both $\{\alpha \mapsto \mathtt{Nat}\}$ and $\{\alpha \mapsto [\beta]\}$, where β is a type and there exists an instance that gives meaning to $\mathtt{eq} : \beta \to \beta \to \mathtt{Bool}$. The intuition here is that we want to be able to compare natural numbers Nat and lists $[\beta]$, given the elements of type β are known to be comparable.

```
class Eq α where
  eq :: α → α → Bool

instance Eq Nat where
  eq x y = x ≐ y
instance Eq β ⇒ Eq [β] where
  eq []       []       = True
  eq (x : xs) (y : ys) = eq x y && eq xs ys

.. eq 42 0 .. eq [42, 0] [42, 0] ..
```

First, typeclass `Eq` is declared with a single generic function signature `eq :: α → α → Bool`. Next, we instantiate `Eq` for {α ↦ `Nat`}. After that, `Eq` is instantiated for {α ↦ `[β]`}, given that an instance `Eq β` can be found. Hence we can call `eq` on expressions with type `Nat` and `[Nat]`. In the latter case, the type constraint `Eq β ⇒ ..` in the instance for lists resolves to the instance for natural numbers.

1.3 Desugaring Typeclass Functionality to System F_O

System F_O is a minimal calculus with support for overloading and polymorphism based on System F. In System F_O we give up high level language constructs and instead work with simple overloaded identifiers.
Using the `decl o in e'` expression we can introduce an new overloaded variable `o`. If declared as overloaded, `o` can be instantiated for type `τ` of expression `e` using the `inst o = e in e'` expression. In Haskell, instances must comply with the generic type signatures defined by the typeclass. Such signatures are not present in System F_O and overloaded variables can be instantiated for arbitrary types. Locally shadowing other instances of the same type is allowed. Constraints can be introduced on the expression level using constraint abstractions `ƛ (o : τ). e'`. Constraint abstractions result in constraint types `[o : τ] ⇒ τ'`. We introduce constraints on the expression level because instance expressions do not have a type annotation in System F_O. Expressions with constraint types `[o : τ] ⇒ τ'` are implicitly treated as expressions of type `τ'` by the type system, given that the constraint `o : τ` can be resolved.

Example: Overloading Equality in System F_O

Recall the Haskell example from above. The same functionality can be expressed in System F_O. For convenience, type annotations for instances are given.

```
decl eq in

inst eq : Nat → Nat → Bool
  = λx. λy. .. in
inst eq : ∀β. [eq : β → β → Bool] ⇒ [β] → [β] → Bool
  = Λβ. ƛ(eq : β → β → Bool). λxs. λys. .. in

.. eq 42 0 .. eq Nat [42, 0] [42, 0] ..
```

First, we declare `eq` to be an overloaded identifier and instantiate `eq` for equality on `Nat`. Next, we instantiate `eq` for equality on lists `[β]`, given that the constraint `eq : β → β → Bool` introduced by the constraint abstraction ƛ is satisfied. Because System F_O is based on System F, we are required to bind type variables using type abstractions Λ and eliminate type variables using type application.
A little caveat: the instance for lists would potentially need to recursively call `eq` for sublists but the formalization of System $F_O$does not actually support recursion. Extending System F_O with recursive let bindings and thus recursive instances is known to be straight forward.

1.4 Translating System F_O back to System F

System F_O can be translated back to System F. Hence, System F_O is not more expressive or powerful than System F. After all, overloading is more of a convenience feature.

We simply could use let bindings with unique variable names and pass constraints as higher order functions.
The Dictionary Passing Transform translates well typed System F_O expressions to well typed System F expressions. The translation requires knowledge acquired during type checking. More specifically, we need to know the instances that were resolved for invocations of overloaded identifiers and the instances that constraints were implicitly resolved to.
The translation removes all `decl o in e` expressions. Instance expressions `inst o = e in e'` are replaced with `let` o_τ `= e in e'` expressions, where o_τ is a unique name with respect to the type `τ` of the expression `e`. Constraint abstractions `ƛ (o : τ). e'` translate to normal abstractions `λ`o_τ`. e'`. Hence, constraint types `[o : τ] ⇒ τ'` translate to function types `τ → τ'`. Invocations of overloaded function names `o` translate to the correct unique variable name o_τ that is bound by the let binding that got introduced by the translation for the instance resolved at that invocation. Implicitly resolved constraints in System F_O must be explicitly passed as arguments in System F. The translation becomes more intuitive when looking at an example.

Example: Dicitionary Passing Transform

Recall the System F_O example from above. We use indices to represent new unique names. Applying the Dictionary Passing Transform to the example above results in a well formed System F expression.

```
let eq₁ : Nat → Nat → Bool
  = λx. λy. .. in
let eq₂ : ∀β. (β → β → Bool) → [β] → [β] → Bool
  = Λβ. λeq₁. λxs. λys. .. in

.. eq₁ 42 0 .. eq₂ Nat eq₁ [42, 0] [42, 0] ..
```

We drop the `decl` expression and transform `inst` definitions to `let` bindings with unique names. Inside the instance for lists, the constraint abstraction translates to a normal lambda abstraction. The lambda abstraction takes the constraint that was implicitly resolved in System F_O as explicit higher order function argument. Invocations of `eq` translate to the correct unique variables eq_i. When eq_2 is invoked for lists of numbers, we must pass the correct instance to eliminate the former constraint abstraction, now higher order function binding, by explicitly passing instance eq_1 as argument.

2 Preliminary

2.1 Dependently Typed Programming in Agda

Agda is a dependently typed programming language and proof assistant [3]. Agda's type system is based on intuitionistic type theory and allows to construct proofs based on the Curry-Howard correspondence. The Curry-Howard correspondence is an isomorphic relationship between programs written in dependently typed languages and mathematical proofs written in first order logic. Because of the Curry-Howard correspondence, programs correspond to proofs and formulae correspond to types. Thus, type checked Agda programs imply the correctness of the corresponding proofs, assuming we do not use unsafe Agda features and Agda is implemented correctly. We will use

Agda to formalize the type preservation proof for the Dictionary Passing Transform from System F_O to System F.

2.2 Design Decisions for the Agda Formalization

To formalize syntaxes in Agda we use a single data type Term indexed by sorts s to represent the syntax. Sorts distinguish between different categories of terms. For example, the sort e_s represents expressions e, τ_s represents types τ and κ_s represents kind. Although, in System F and System F_O there only exists a single kind $\star$. The idea of sorts originates from the theory of pure type systems [2], but neither System F nor System F_O allow any interesting dependencies between terms of the sort e_s, τ_s, and κ_s. Using a single data type to formalize the syntax yields more elegant proofs involving contexts, substitutions and renamings. In consequence of using a single data type, we must use extrinsic typing because intrinsically typed terms Term e_s ⊢ Term τ_s would need to be indexed by themselves and Agda does not support self-indexed data types. In the actual implementation, Term has another index S that we will ignore for now.

2.3 Overview of the Type Preservation Proof

The overall goal will be to prove that the Dictionary Passing Transform is type preserving. Let $\vdash t$ be any well formed System F_O term $\Gamma \vdash_{F_O} t : T$, where Γ is a typing environment of type Ctx_{F_O}, t is a $\mathsf{Term}_{F_O}\ s$, T is a $\mathsf{Term}_{F_O}\ s'$ and s' is the sort of the typing result for terms of the sort s. There exist two cases for typings: $\Gamma \vdash e : \tau$ and $\Gamma \vdash \tau : \star$. Let $\rightsquigarrow : (\Gamma \vdash_{F_O} t : T) \to \mathsf{Term}_F\ s$ be the Dictionary Passing Transform that translates well typed System F_O terms to untyped System F terms. Further, let $\rightsquigarrow_\Gamma : \mathsf{Ctx}_{F_O} \to \mathsf{Ctx}_F$ be the transform of contexts and $\rightsquigarrow_T : \mathsf{Term}_{F_O}\ s' \to \mathsf{Term}_F\ s'$ be the transform of untyped types and kinds. We show that for all well typed System F_O terms $\vdash t$ the Dictionary Passing Transform results in a well typed System F term $(\rightsquigarrow_\Gamma \Gamma) \vdash_F (\rightsquigarrow \vdash t) : (\rightsquigarrow_T\ T)$.

We begin by formalizing the syntax, typing and semantic of System F in Agda and prove its soundness in section 3. In section 4, we formalize System F_O's syntax and typing. In the end, we formalize the translation of the Dictionary Passing Transform and prove it to be type preserving in section 5.

3 System F

3.1 Specification

Sorts

The formalization of System F requires three sorts: e_s for expressions, τ_s for types and κ_s for kinds.

```
data Sort : Bindable → Set where
  eₛ : Sort ⊤ᴮ
  τₛ : Sort ⊤ᴮ
  κₛ : Sort ⊥ᴮ
```

Sorts are indexed by the boolean data type Bindable. The index $\top^B$ indicates that variables for terms of a sort can be bound. In contrast, $\bot^B$ says that variables for terms of a sort cannot be bound. In this case, System F supports abstracting over expressions and types, but not over kinds. Going forward, we will use the variable s for sorts and the variable S for lists of bindable sorts with type Sorts = List (Sort $\top^B$).

Syntax

The syntax of System F is represented in a single data type Term, indexed by sorts S and sort s. The index S is inspired by Debruijn indices. Debruijn indices reference variables using a number that counts the amount of binders that are in scope between the binding of the variable and the position it is used at. In Agda, terms are often indexed by the amount of bound variables. The variable constructor then only accepts Debruijn indices that are smaller or equal to the current amount of bound variables. Thus, unbound variables cannot be referenced by definition. This technique is also referred to as intrinsically scoped. But indexing Term with a number is not sufficient because System F has both expression variables and type variables that need to be distinguished. To solve this problem, we need to extend the idea of Debruijn indices and store the corresponding sort for each variable. Thus, we let S be a list of sorts instead of a number. The length of S represents the amount of bound variables and the elements s_i of the list represent the sort of the variable bound at debruijn index i. The index s represents the sort of the term itself.

```
data Term : Sorts → Sort r → Set where
  `_          : s ∈ S → Term S s
  tt          : Term S eₛ
  λ`x→_       : Term (S ▷ eₛ) eₛ → Term S eₛ
  Λ`α→_       : Term (S ▷ τₛ) eₛ → Term S eₛ
  _·_         : Term S eₛ → Term S eₛ → Term S eₛ
  _•_         : Term S eₛ → Term S τₛ → Term S eₛ
  let`x=_`in_ : Term S eₛ → Term (S ▷ eₛ) eₛ → Term S eₛ
  `⊤          : Term S τₛ
  _⇒_         : Term S τₛ → Term S τₛ → Term S τₛ
  ∀`α_        : Term (S ▷ τₛ) τₛ → Term S τₛ
  ⋆           : Term S κₛ
```

Variables ` x are represented as membership proofs of type $s \in S$. Membership proofs are inductively defined, similar to the definition of natural numbers. Membership proofs can be constructed using the constructor here refl, where refl is proof that the last element in S is the element we searched for. Alternatively, membership proofs can be constructed via the constructor there x, where x is another membership proof for S with one element less. In consequence, we can only reference already bound variables by definition.
The unit element tt and unit type `⊤ represent base expressions and types respectively. Lambda abstractions λ`x→ e' result in function types $\tau_1 \Rightarrow \tau_2$ and type abstractions Λ`α→ $e$' result in forall types ∀`α τ'. Both abstractions introduce an additional sort e_s, or τ_s respectively, to the index S of the body e' to account for the newly bound variable.
The application constructor $e_1 \cdot e_2$ applies the argument e_2 to the function e_1.
Similarly, type application $e \bullet \tau$ eliminates type abstractions.

Let bindings let‘x= e_2 ‘in e_1 combine abstraction and application.
The kind ⋆ is kind of all types.
We use abbreviations Var S s = $s \in S$, Expr S = Term S e_s, Type S = Term S τ_s and variables x, e and τ respectively. Furthermore, we use the variable t for an arbitrary Term S s.

Renaming

Renamings ρ of type Ren S_1 S_2 are defined as total functions that map variables Var S_1 s to variables Var S_2 s. Renamings preserve the sort s of the variable.

```
Ren : Sorts → Sorts → Set
Ren S₁ S₂ = ∀ {s} → Var S₁ s → Var S₂ s
```

Applying a renaming Ren S_1 S_2 to a term Term S_1 s yields a new term Term S_2 s, where variables are represented as references to elements in S_2 instead of S_1.

```
ren : Ren S₁ S₂ → (Term S₁ s → Term S₂ s)
ren ρ (‘ x) = ‘ (ρ x)
ren ρ (λ‘x→ e) = λ‘x→ (ren (extᵣ ρ) e)
ren ρ (τ₁ ⇒ τ₂) = ren ρ τ₁ ⇒ ren ρ τ₂
- ...
```

The renaming is applied to all variables x.
When we encounter a binder for a term of sort s, the renaming is extended, using function ext$_r$.

```
extᵣ : Ren S₁ S₂ → Ren (S₁ ▷ s) (S₂ ▷ s)
extᵣ ρ (here refl) = here refl
extᵣ ρ (there x) = there (ρ x)
```

The extension of a renaming introduces an additional variable of sort s. Thus, if we encounter the new binding here refl in the extended renaming, then we return the variable for the new binding here refl. The variables x of the original renaming ρ are weakened by wrapping them in an additional there constructor.
The weakening of a term can be defined as shifting all variables by one.

```
wk : Term S s → Term (S ▷ s’) s
wk = ren there
```

Because variables are represented as membership proofs, shifting variables by one binder is accomplished by wrapping them in an additional there constructor.

Substitution

The definition of substitutions σ with type Sub S_1 S_2 is similar to the definition of renamings. But rather than mapping variables to variables, substitutions map variables to terms.

```
Sub : Sorts → Sorts → Set
Sub S₁ S₂ = ∀ s → Var S₁ s → Term S₂ s
```

Applying a substitution using the sub function is analogous to applying a renaming using ren. If we encounter a binder in sub, the substitution must be extended using function ext_s.

$$\mathsf{ext}_s : \mathsf{Sub}\ S_1\ S_2 \to (s : \mathsf{Sort}\ \top^B) \to \mathsf{Sub}\ (S_1 \triangleright s)\ (S_2 \triangleright s)$$
$$\mathsf{ext}_s\ \sigma\ s\ \_\ (\mathsf{here\ refl}) = \text{`}\ \mathsf{here\ refl}$$
$$\mathsf{ext}_s\ \sigma\ s\ \_\ (\mathsf{there}\ x) = \mathsf{wk}\ (\sigma\ \_\ x)$$

For the newly introduced binder of variable here refl, we return the variable term ‘ here refl. Furthermore, all terms originally present in the substitution σ are weakened using the function wk that itself uses renaming to shift all variables in the term by one recursively.
The substitution operator t [t'] substitutes the last bound variable in t with t', given that the sort of the last binder corresponds to the sort of term t'.

$$\_[\_] : \mathsf{Term}\ (S \triangleright s')\ s \to \mathsf{Term}\ S\ s' \to \mathsf{Term}\ S\ s$$
$$t\ [\ t'\ ] = \mathsf{sub}\ (\mathsf{single}_s\ \mathsf{id}_s\ t')\ t$$

A single substitution $\mathsf{single}_s : \mathsf{Sub}\ S_1\ S_2 \to \mathsf{Term}\ S_2\ s \to \mathsf{Sub}\ (S_1 \triangleright s)\ S_2$ takes an existing substitution σ' and substitutes t' for an additional new binding. In the case of _[_], we let σ' be the identity substitution $\mathsf{id}_s : \mathsf{Sub}\ S\ S$.

Context

Similar to terms, typing contexts Γ of type Ctx S are indexed by the list of bound variables as well. In consequence, only types and kinds for bound variables can be stored in Γ by definition.

```
data Ctx : Sorts → Set where
  ∅ : Ctx []
  _▶_ : Ctx S → Term S (type-of s) → Ctx (S ▷ s)
```

Contexts are inductively defined and can either be empty $\emptyset$ or extended with one element T, using the constructor $\Gamma \blacktriangleright T$. The variable T represents terms of the sort type-of s. The function type-of maps bindable sorts s to the sort of the term that is stored in Γ for variables of the sort s.

$$\mathsf{type\text{-}of}\ \mathsf{e}_s = \tau_s$$
$$\mathsf{type\text{-}of}\ \tau_s = \kappa_s$$

Expression variables require Γ to store the corresponding type. For type variables, Γ stores the corresponding kind. Thus, if we bind a new variable for a term of the sort s, the context Γ needs to be extended by a term of the sort type-of s.
The lookup function resolves the type or kind for a variable x in Γ.

$$\mathsf{lookup} : \mathsf{Ctx}\ S \to \mathsf{Var}\ S\ s \to \mathsf{Term}\ S\ (\mathsf{type\text{-}of}\ s)$$
$$\mathsf{lookup}\ (\Gamma \blacktriangleright T)\ (\mathsf{here\ refl}) = \mathsf{wk}\ T$$
$$\mathsf{lookup}\ (\Gamma \blacktriangleright T)\ (\mathsf{there}\ x) = \mathsf{wk}\ (\mathsf{lookup}\ \Gamma\ x)$$

Both the base and induction case wrap the looked up constraint in a weakening. Thus, the looked up T has index S that aligns with the current amount of bound variables. The lookup function cannot fail by definition because we only allow to lookup bound variables that must have an entry in Γ.

Typing

The typing relation $\Gamma \vdash t : T$ relates terms t to their typing result T in a context Γ.

```
data _⊢_:_ : Ctx S → Term S s → Term S (type-of s) → Set where
  ⊢`x :
    lookup Γ x ≡ τ →
    Γ ⊢ ` x : τ
  ⊢⊤ :
    Γ ⊢ tt : `⊤
  ⊢λ :
    Γ ▶ τ ⊢ e : wk τ' →
    Γ ⊢ λ`x→ e : τ ⇒ τ'
  ⊢Λ :
    Γ ▶ ⋆ ⊢ e : τ →
    Γ ⊢ Λ`α→ e : ∀`α τ
  ⊢· :
    Γ ⊢ e₁ : τ₁ ⇒ τ₂ →
    Γ ⊢ e₂ : τ₁ →
    Γ ⊢ e₁ · e₂ : τ₂
  ⊢• :
    Γ ⊢ e : ∀`α τ →
    Γ ⊢ e • τ' : τ [ τ' ]
  ⊢let :
    Γ ⊢ e₂ : τ →
    Γ ▶ τ ⊢ e₁ : wk τ' →
    Γ ⊢ let`x= e₂ `in e₁ : τ'
  ⊢τ :
    Γ ⊢ τ : ⋆
```

The rule ⊢\`x says that a variable \` x has type τ, if the type for x in Γ is τ.
All unit expressions tt have type \`⊤. This is expressed by the rule ⊢⊤.
The rule for abstractions ⊢λ introduces an expression variable of type τ to the body e. Because the resulting body type τ' cannot use the newly introduced expression variable, we let τ' have one variable bound less and weaken it to align with the context Γ ▶ τ. Hence, τ' aligns with τ in the list of bound variables to form the resulting function type $\tau \Rightarrow \tau$'.
The type abstraction rule ⊢Λ introduces a type variable to the body e and results in the forall type ∀\`α τ, where τ is the type of e. The type variable in e is introduced by extending Γ with the kind $\star$.
Application is handled by the rule ⊢·. The rule says that if e_1 is a function from τ_1 to τ_2 and e_2 has type τ_1, then $e_1 \cdot e_2$ has type τ_2.
Similarly, the type application rule ⊢• states that if e has type ∀\`α τ, then a can be substituted with another type τ' inside τ.
The rule ⊢let combines the abstraction and application rule.
Regarding the typing of types, the rule ⊢τ indicates that all types τ are well formed and have kind $\star$. Type variables are correctly typed per definition and type constructors ∀\`α and ⇒ accept arbitrary types as their arguments. Hence, all types are well typed.

Typing of Renaming & Substitution

Because of extrinsic typing, both renamings and substitutions need to have typed counterparts.
We formalize typed renamings $\vdash\rho$ inductively as order preserving embeddings. Thus, if a variable x_1 of type $s_1 \in S_1$ references an element with an index smaller than some other variable x_2 in S_1, then renamed x_1 must still reference an element with a smaller index than renamed x_2 in S_2. Arbitrary renamings would allow swapping items and potentially violate the telescoping. Telescoping allows types stored in the context to depend on type variables bound before them.
Interestingly, because of the intrinsically scoped definition of terms, all renamings must be order preserving embeddings by definition. Thus, it should be possible to prove order preservation in the form of lemmas. Instead we choose to represent the rules for order preserving embeddings as constructors of a data type, such that we can access the property of order preservation by matching on the data type.

```
data _:_⇒ᵣ_ : Ren S₁ S₂ → Ctx S₁ → Ctx S₂ → Set where
  ⊢idᵣ : ∀ {Γ} → _:_⇒ᵣ_ {S₁ = S} {S₂ = S} idᵣ Γ Γ
  ⊢extᵣ : ∀ {ρ : Ren S₁ S₂} {Γ₁ : Ctx S₁} {Γ₂ : Ctx S₂}
              {T' : Term S₁ (type-of s)} →
    ρ : Γ₁ ⇒ᵣ Γ₂ →
    (extᵣ ρ) : (Γ₁ ▶ T') ⇒ᵣ (Γ₂ ▶ ren ρ T')
  ⊢dropᵣ : ∀ {ρ : Ren S₁ S₂} {Γ₁ : Ctx S₁} {Γ₂ : Ctx S₂}
               {T' : Term S₂ (type-of s)} →
    ρ : Γ₁   ⇒ᵣ Γ₂ →
    (dropᵣ ρ) : Γ₁ ⇒ᵣ (Γ₂ ▶ T')
```

The identity renaming ⊢id_r is typed by definition.
The typed extension of a renaming ⊢ext_r allows to extend both Γ_1 and Γ_2 by T' and renamed T' respectively. The constructor ⊢ext_r corresponds to the typed version of the function ext_r that is used when a binder is encountered.
The constructor ⊢drop_r allows to introduce T' only in Γ_2. Hence, ⊢drop_r ⊢id_r corresponds to the typed weakening of a term.
Typed Substitutions are defined as total functions, similar to untyped substitutions.

```
_:_⇒ₛ_ : Sub S₁ S₂ → Ctx S₁ → Ctx S₂ → Set
_:_⇒ₛ_ {S₁ = S₁} σ Γ₁ Γ₂ = ∀ {s} (x : Var S₁ s) →
                                   Γ₂ ⊢ σ _ x : (sub σ (lookup Γ₁ x))
```

Typed substitutions $\vdash\sigma$ map variables $x \in S_1$ to the corresponding typing of the term $\sigma\ x$ in Γ_2. The type of the term $\sigma\ x$ must be the original type of x in Γ_1 applied to the substitution σ.

Semantics

The semantics of System F are formalized as call-by-value, that is, there is no reduction under binders.
Values are indexed by their corresponding irreducible expression.

```
data Val : Expr S → Set where
  v-λ : Val (λ`x→ e)
```

```
v-Λ : Val (Λ‘α→ e)
v-tt : ∀ {S} → Val (tt {S = S})
```

System F has three values. The two closure values v-λ and v-Λ and the unit value v-tt. We formalize small step semantics where each constructor represents a single reduction step $e \hookrightarrow e'$. We distinguish between β and ξ rules. Meaningful computation in the form of substitution is done by β rules while ξ rules only reduce subexpressions.

```
data _↪_ : Expr S → Expr S → Set where
  β-λ :
    Val e₂ →
    (λ‘x→ e₁) · e₂ ↪ e₁ [ e₂ ]
  β-Λ :
    (Λ‘α→ e) • τ ↪ e [ τ ]
  β-let :
    Val e₂ →
    let‘x= e₂ ‘in e₁ ↪ (e₁ [ e₂ ])
  ξ-·₁ :
    e₁ ↪ e →
    e₁ · e₂ ↪ e · e₂
  ξ-·₂ :
    e₂ ↪ e →
    Val e₁ →
    e₁ · e₂ ↪ e₁ · e
  ξ-• :
    e ↪ e’ →
    e • τ ↪ e’ • τ
  ξ-let :
    e₂ ↪ e →
    let‘x= e₂ ‘in e₁ ↪ let‘x= e ‘in e₁
```

The rules β-λ and β-Λ give meaning to application and type application by substituting the applied expression, or type respectively, into the abstraction body. In both cases, we make sure that the abstraction and applied argument must be a irreducible.
The reduction rule β-let is equivalent to β-λ and substitutes value e_2 into e_1.
The rules ξ-·$_i$ and ξ-• evaluate subexpressions of applications until e_1 and e_2, or e respectively, are values.
The rule ξ-let reduces the bound expression e_2 until e_2 is a value and β-let can be applied.

3.2 Soundness

Progress

We prove progress by showing that a typed expression e can either be further reduced to another expression e' or e is a value. The proof follows by induction over the typing rules.

```
progress :
  ∅ ⊢ e ⦂ τ →
  (∃[ e’ ] (e ↪ e’)) ⊎ Val e
```

```
progress ⊢⊤ = inj₂ v-tt
progress (⊢λ _) = inj₂ v-λ
progress (⊢Λ _) = inj₂ v-Λ
progress (⊢· {e₁ = e₁} {e₂ = e₂} ⊢e₁ ⊢e₂) with progress ⊢e₁ | progress ⊢e₂
... | inj₁ (e₁ ' , e₁↪e₁ ') | _ = inj₁ (e₁ ' · e₂ , ξ-·₁ e₁↪e₁ ')
... | inj₂ v | inj₁ (e₂ ' , e₂↪e₂ ') = inj₁ (e₁ · e₂ ' , ξ-·₂ e₂↪e₂ ' v)
... | inj₂ (v-λ {e = e₁}) | inj₂ v = inj₁ (e₁ [ e₂ ] , β-λ v)
progress (⊢• {τ' = τ'} ⊢e) with progress ⊢e
... | inj₁ (e' , e↪e') = inj₁ (e' • τ' , ξ-• e↪e')
... | inj₂ (v-Λ {e = e}) = inj₁ (e [ τ' ] , β-Λ)
progress (⊢let {e₂ = e₂} {e₁ = e₁} ⊢e₂ ⊢e₁) with progress ⊢e₂
... | inj₁ (e₂ ' , e₂↪e₂ ') = inj₁ ((let`x= e₂ ' `in e₁) , ξ-let e₂↪e₂ ')
... | inj₂ v = inj₁ (e₁ [ e₂ ] , β-let v)
```

The cases ⊢⊤, ⊢λ and ⊢Λ result in values. The application cases ⊢·, ⊢• and ⊢let follow directly from the induction hypothesis.

Subject Reduction

We prove subject reduction, that is, reduction preserves typing. More specifically, an expression e with type τ still has type τ after being reduced to e'. We prove subject reduction by induction over the reduction rules.

```
subject-reduction : ∀ {Γ : Ctx S} →
  Γ ⊢ e : τ →
  e ↪ e' →
  Γ ⊢ e' : τ
subject-reduction (⊢· (⊢λ ⊢e₁) ⊢e₂) (β-λ v₂) = e[e]-preserves ⊢e₁ ⊢e₂
subject-reduction (⊢· ⊢e₁ ⊢e₂) (ξ-·₁ e₁↪e) = ⊢· (subject-reduction ⊢e₁ e₁↪e) ⊢e₂
subject-reduction (⊢· ⊢e₁ ⊢e₂) (ξ-·₂ e₂↪e x) = ⊢· ⊢e₁ (subject-reduction ⊢e₂ e₂↪e)
subject-reduction (⊢• (⊢Λ ⊢e)) β-Λ = e[τ]-preserves ⊢e ⊢τ
subject-reduction (⊢• ⊢e) (ξ-• e↪e') = ⊢• (subject-reduction ⊢e e↪e')
subject-reduction (⊢let ⊢e₂ ⊢e₁) (β-let v₂) = e[e]-preserves ⊢e₁ ⊢e₂
subject-reduction (⊢let ⊢e₂ ⊢e₁) (ξ-let e₂↪e') = ⊢let
  (subject-reduction ⊢e₂ e₂↪e') ⊢e₁
```

The ξ reduction cases ξ-·₁, ξ-·₂, ξ-• and ξ-let follow directly from the induction hypothesis.
For the β reduction cases β-λ, β–Λ and β-let we need to prove that substitutions preserve the typing. We have two different types of substitution present inside the reduction rules: e [e] and e [τ]. Both e[e]-preserves and e[τ]-preserves follow from a more general lemma ⊢σ-preserves. The lemma ⊢σ-preserves proves that all typed substitutions preserve typing.

```
⊢σ-preserves : ∀ {σ : Sub S₁ S₂} {Γ₁ : Ctx S₁} {Γ₂ : Ctx S₂}
                 {t : Term S₁ s} {T : Term S₁ (type-of s)} →
  σ : Γ₁ ⇒ₛ Γ₂ →
  Γ₁ ⊢ t : T →
  Γ₂ ⊢ (sub σ t) : (sub σ T)
```

The lemma ⊢σ-preserves follows by induction over the typing rules and lemmas about the type preservation of substitutions and renamings. More specifically, we need to prove that all operations on substitutions preserve the typing as well. For instance, we need to prove that the extension of a substitution ext_s, that itself uses renaming under the hood, is type preserving. Thus, we also need to prove that renamings are type preserving. [1]. The soundness property of System F follows as a consequence of progress and subject-reduction.

4 System $\mathrm{F_O}$

4.1 Specification

Sorts

In addition to the sorts of System F, System $\mathrm{F_O}$ introduces two new sorts: o_s for overloaded variables and c_s for constraints.

```
data Sort : Bindable → Set where
  oₛ : Sort ⊤ᴮ
  cₛ : Sort ⊥ᴮ
  - ...
```

Terms of sort o_s can only be constructed using the variable constructor ‘_. Thus, terms of sort o_s are called overloaded variables. We use the variable o for overloaded variables and variable c for constraints. Variables for constraints do not exist in System $\mathrm{F_O}$ and thus c_s is indexed by $\bot^B$.

Syntax

We only discuss additions to the syntax of System F.

```
data Term : Sorts → Sort r → Set where
  decl‘o‘in_       : Term (S ▷ oₛ) eₛ → Term S eₛ
  inst‘_‘=_‘in_ : Term S oₛ → Term S eₛ → Term S eₛ → Term S eₛ
  _:_              : Term S oₛ → Term S τₛ → Term S cₛ
  ƛ_⇒_             : Term S cₛ → Term S eₛ → Term S eₛ
  [_]⇒_            : Term S cₛ → Term S τₛ → Term S τₛ
  - ...
```

Declarations decl‘o‘in e introduce a new overloaded variable o. Hence, S is extended by sort o_s inside the body e.
The expression inst‘ $o = e_2$ ‘in e_1 introduces an additional instance for o. The actual meaning for the instance is given by e_2. Instance expressions do not introduce new bindings and thus, the index S is never extended.
Constraints c can be constructed using constructor $o : \tau$.
A constraint c can be part of a constraint abstraction $\lambda\ c \Rightarrow e$. Constraint abstractions assume the constraint c to be valid inside the body e and result in constraint types $[\ c\ ]\Rightarrow \tau$. The constraint type lifts the constraint from the expression level to the type level, where it will be implicitly eliminated by the typing rules.
Going forward, we will use the abbreviation $\mathsf{Cstr}\ S = \mathsf{Term}\ S\ \mathsf{c}_s$.

[1] The soundness proof for System F is not the main part of this work and thus, the explanation is rather short. The full proof can be found on GitHub: `https://github.com/Mari-W/System-Fo/blob/main/proofs/SystemF.agda`

Renaming & Substitution

Renamings and substitutions in System F_O are formalized identically to renamings and substitutions in System F. The only difference is that we define the substitution operator only on types.

```
_[_] : Type (S ▷ τs) → Type S → Type S
τ [ τ' ] = sub (single-types ids τ') τ
```

Because we do not formalize semantics for System F_O, only substitutions of types in types are necessary. Type in type substitution appears in the typing rule for type application.

Context

In addition to normal context items, the existence of overloaded variables is stored inside the context. Overloaded variables act as normal context items. Because overloaded variables themselves do not have a type, but rather multiple types that they can take on, we only need to store their existence in Γ. Thus, similar to type variables, we store kind $\star$ in Γ to denote the existence of an overloaded variable. As a result, the type-of function is extended and returns the sort κ_s when applied to the sort o_s.
The types that an overloaded variable can take on are stored in the form of constraints. Constraints can be introduced to the context by both constraint abstractions and instance expressions.

```
data Ctx : Sorts → Set where
  _▸_ : Ctx S → Cstr S → Ctx S
  - ...
```

We write Γ ▸ c to pick up a constraint c. Constraints give an additional meaning to an overloaded variable that is already bound. Hence index S is not modified.
The lookup function in System F_O is defined analogously to lookup in System F and simply ignores constraints stored in the context.

Constraint Solving

The search for constraints in a context is formalized analogously to membership proofs $s \in S$. The subtle difference is that we reference constraints in Γ and not in S.

```
data [_]∈_ : Cstr S → Ctx S → Set where
  here : [ (' o : τ) ]∈ (Γ ▸ (' o : τ))
  under-bind : {I : Term S (item-of s')} →
    [ (' o : τ) ]∈ Γ → [ (' there o : wk τ) ]∈ (Γ ▶ I)
  under-cstr : [ c ]∈ Γ → [ c ]∈ (Γ ▸ c')
```

The here constructor is analogous to the here constructor of memberships and can be used when the last item in Γ is the desired constraint c.
If the last item in the context is not the desired constraint c, then c must be further inside the context. The constraint can either behind a item stored in Γ (under-bind) or a constraint (under-cstr). In the case that c is under a binder, the constraint needs to be weakened, to align in S with the position it is resolved for.

Typing

We only discuss typing rules not already discussed in the System F specification.

```
data _⊢_:_ : Ctx S → Term S s → Term S (type-of s) → Set where
  ⊢‘o :
    [ ‘ o : τ ]∈ Γ →
    Γ ⊢ ‘ o : τ
  ⊢λ :
    Γ ▸ c ⊢ e : τ →
    Γ ⊢ λ c ⇒ e : [ c ]⇒ τ
  ⊢⊘ :
    Γ ⊢ e : [ ‘ o : τ ]⇒ τ’ →
    [ ‘ o : τ ]∈ Γ →
    Γ ⊢ e : τ’
  ⊢decl :
    Γ ▶ ⋆ ⊢ e : wk τ →
    Γ ⊢ decl‘o‘in e : τ
  ⊢inst :
    Γ ⊢ e₂ : τ →
    Γ ▸ (‘ o : τ) ⊢ e₁ : τ’ →
    Γ ⊢ inst‘ ‘ o ‘= e₂ ‘in e₁ : τ’
  - ...
```

The rule for overloaded variables ⊢‘o says that if we can resolve the constraint o : τ in Γ, then o can take on type τ.
The rule for constraint abstraction ⊢λ appends the constraint c to Γ and thus assumes c to be valid inside the body e. Constraint abstractions result in the corresponding constraint type [c]⇒ τ that lifts the constraint onto the type level.
Expressions e with constraint type [c]⇒ τ’ have the constraint implicitly eliminated using the ⊢⊘ rule, given c can be resolved in Γ. Because the rule can be applied to arbitrary e, it is not syntax directed.
The rule ⊢decl introduces a new overloaded variable o to e. To introduce o in Γ, we only need to store the information that o exists as overloaded variable. The existence of o is denoted by extending Γ with kind ⋆. The types that o can take on, will be stored inside constraints. Analogous to the type τ’ inside the abstraction rule ⊢λ, the resulting type τ is weakened to align in S with Γ not extended by ⋆, such that it can act as the resulting type of the typing.
An instance for an overloaded variable o is typed using the rule ⊢inst. We extend Γ with constraint o : τ inside e_1, where τ is the type of e_2.

Typing Renaming & Substitution

Typed renamings are identical to typed renamings in System F, except there is an additional case for the weakening by a constraint.

```
data _:_⇒ᵣ_ : Ren S₁ S₂ → Ctx S₁ → Ctx S₂ → Set where
  ⊢drop-cstrᵣ : ∀ {Γ₁ : Ctx S₁} {Γ₂ : Ctx S₂} {τ} {o} →
    ρ : Γ₁ ⇒ᵣ Γ₂ →
    ρ : Γ₁ ⇒ᵣ (Γ₂ ▸ (o : τ))
  - ...
```

Constraint o : τ can be introduced only to Γ_2 using the $\vdash$drop-cstr$_r$ constructor. Dropping a constraint corresponds to a typed weakening, similar to constructor $\vdash$drop$_r$, but instead of introducing an unused variable we introduce an unused constraint.
Other than in System F, arbitrary substitutions will not be allowed in System F_O. Similar to the substitution operator we restrict typed substitutions in System F_O to substitutions of types in types.

```
data _:_⇒s_ : Sub S1 S2 → Ctx S1 → Ctx S2 → Set where
  ⊢types : ∀ {Γ1 : Ctx S1} {Γ2 : Ctx S2} {τ : Type S2} →
    σ : Γ1 ⇒s Γ2 →
    single-types σ τ : Γ1 ▶ ⋆ ⇒s Γ2
  - ...
```

The constructor $\vdash$type$_s$ allows to introduce an additional new type variable binder that is substituted with type τ. Thus, $\vdash$type$_s$ complements the single-type$_s$ function. The intuition here is that if we would allow all terms to be introduced using a $\vdash$term$_s$ constructor, then typed substitutions in System F_O would be arbitrary again. The restriction to type in type substitutions simplifies the type preservation proof for the Dictionary Passing Transform by eliminating cases for non-type terms that would otherwise needed to be proven. Constructors $\vdash$id$_s$, $\vdash$ext$_s$, $\vdash$drop$_s$ and $\vdash$drop-cstr$_s$ are not shown. All of them function the same way as their counterparts in typed renamings.

5 The Dictionary Passing Transform

5.1 Translation

Sorts

The translation of System F_O sorts to System F sorts only considers sorts that are bindable. The two missing non-bindable sorts c$_s$ and κ$_s$ do not need to be translated. Intuitively there does not even exist a sensible translation for c$_s$.

```
s⇝s : F^O.Sort ⊤^B → F.Sort ⊤^B
s⇝s es = es
s⇝s os = es
s⇝s τs = τs
```

Sorts e$_s$ and τ$_s$ translate to their corresponding counterparts in System F.
Overloaded variables in System F_O translate to normal variables in System F. Thus the sort o$_s$ translates to e$_s$.
Translating lists S directly is not possible because there might appear additional sorts inside the list after the translation. New sorts must be added for variable bindings introduced by the translation. For example, a inst‘ ‘ $o = e_2$ ‘in e_1 expression does not bind a new variable in e_1, but translates to a let‘x= e_2 ‘in e_1 binding. Hence S must have an additional entry e$_s$ at the corresponding position to further function as valid index for the translated e_1. To solve this problem the System F_O context Γ is used to build the translated S. The context stores the relevant information about introduced constraints and thus where new bindings will occur that were not present in System F_O.

```
Γ⇝S : F^O.Ctx F^O.S → F.Sorts
Γ⇝S ∅ = []
Γ⇝S (Γ ▸ c) = Γ⇝S Γ ▷ F.e_s
Γ⇝S {S ▷ s} (Γ ▶ x) = Γ⇝S Γ ▷ s⇝s s
```

The empty context $\emptyset$ corresponds to the empty list [].
For each constraint in Γ an additional sort e_s is appended to S.
If we find that a normal item is stored in the context, the sort s is directly translated using the function s⇝s.

Variables

Similar to lists S, the translation for variables x needs context information.

```
x⇝x : ∀ {Γ : F^O.Ctx F^O.S} →
  F^O.Var F^O.S F^O.s → F.Var (Γ⇝S Γ) (s⇝s F^O.s)
x⇝x {Γ = Γ ▶ τ} (here refl) = here refl
x⇝x {Γ = Γ ▶ τ} (there x) = there (x⇝x x)
x⇝x {Γ = Γ ▸ c} x = there (x⇝x x)
```

If an item is stored in the context we can translate the variable directly.
Whenever a constraint is encountered, x is wrapped in an additional there. This is because the expression that introduced the constraint will translate to an expression with an additional new binding that needs to be respected in System F.
Furthermore, resolved constraints translate to correct unique expression variables. We can apply the same idea as seen in the translation for variables because the type for resolved constraints [c]$\in \Gamma$ preserves the structure of the context perfectly.

```
o:τ∈Γ⇝x : ∀ {Γ : F^O.Ctx F^O.S} →
  [ ‘ F^O.o : F^O.τ ]∈ Γ → F.Var (Γ⇝S Γ) F.e_s
o:τ∈Γ⇝x here = here refl
o:τ∈Γ⇝x (under-bind o:τ∈Γ) = there (o:τ∈Γ⇝x o:τ∈Γ)
o:τ∈Γ⇝x (under-cstr o:τ∈Γ) = there (o:τ∈Γ⇝x o:τ∈Γ)
```

Inside the base base case we found the correct instance, now variable.
When we encounter a normal binding in the case under-bind, we wrap the applied induction hypothesis in the there constructor to respect the binding.
In the induction case under-cstr we again wrap the applied induction hypothesis in an additional there that was not present before.

Context

The translation of contexts is mostly a direct translation. We only look at the translation of constraints stored in the context.

```
Γ⇝Γ : (Γ : F^O.Ctx F^O.S) → F.Ctx (Γ⇝S Γ)
Γ⇝Γ (Γ ▸ (‘ o : τ)) = (Γ⇝Γ Γ) ▶ τ⇝τ τ
- ...
```

Following the idea from above, constraints $o : \tau$ stored inside Γ translate to normal items in the translated Γ. The item introduced is the translated type τ⇝τ τ that was originally required by the constraint. This is exactly what we want because for each constraint in System F_O there will be an additional binder in System F that accepts the constraint as higher order function. Thus, the corresponding function type for that binding is expected in Γ at that position.

Renaming & Substitution

Typed renamings in System F_O translate to untyped renamings in System F.

```
⊢ρ⇝ρ : ∀ {ρ : F^O.Ren F^O.S₁ F^O.S₂} {Γ₁ : F^O.Ctx F^O.S₁} {Γ₂ : F^O.Ctx F^O.S₂} →
  ρ F^O.: Γ₁ ⇒ᵣ Γ₂ →
  F.Ren (Γ⇝S Γ₁) (Γ⇝S Γ₂)
⊢ρ⇝ρ (⊢drop-cstrᵣ ⊢ρ) = F.dropᵣ (⊢ρ⇝ρ ⊢ρ)
- ...
```

Because constraints in contexts translate to actual bindings, the constructor $\vdash$drop-cstr$_r$ translates to drop$_r$ in System F.
Typed renamings $\vdash$id$_r$, $\vdash$ext$_r$ and $\vdash$drop$_r$ translate to their untyped counterparts.
The translation of typed substitutions to untyped substitutions follows similarly.

```
⊢σ⇝σ : ∀ {σ : F^O.Sub F^O.S₁ F^O.S₂} {Γ₁ : F^O.Ctx F^O.S₁} {Γ₂ : F^O.Ctx F^O.S₂} →
  σ F^O.: Γ₁ ⇒ₛ Γ₂ →
  F.Sub (Γ⇝S Γ₁) (Γ⇝S Γ₂)
⊢σ⇝σ (⊢typeₛ {τ = τ} ⊢σ) = F.singleₛ (⊢σ⇝σ ⊢σ) (τ⇝τ τ)
- ...
```

The typed renaming $\vdash$type$_s$ translates to its untyped counterpart for arbitrary terms single$_s$.
The cases $\vdash$id$_s$, $\vdash$ext$_s$, $\vdash$drop$_s$ and $\vdash$drop-cstr$_s$ are analogous to the cases for renamings.

Terms

Types and kinds can be translated without typing information. Kind $\star$ translates to its direct counterpart in System F. Furthermore, all System F_O types translate to their direct counterpart in System F, except the constraint type [o : τ]⇒ τ'.

```
τ⇝τ : ∀ {Γ : F^O.Ctx F^O.S} →
  F^O.Type F^O.S →
  F.Type (Γ⇝S Γ)
τ⇝τ ([ o : τ ]⇒ τ') = τ⇝τ τ ⇒ τ⇝τ τ'
- ...
```

Constraint types [o : τ]⇒ τ' translate to function types $\tau \Rightarrow \tau$'. The translation from constraint types to function types corresponds directly to the translation of constraint abstractions to normal abstractions. The implicitly resolved constraint will be taken as higher order function argument of type τ.
Arbitrary terms can only be translated using typing information. The typing carries information about the instances that were resolved for usages of overloaded variables and the instances that were implicitly resolved for constraints. We only look at the

translation of System $\mathrm{F_O}$ expressions that do not have a direct counterpart in System F.

```
⊢t⇝t : ∀ {Γ : F^O.Ctx F^O.S} {t : F^O.Term F^O.S F^O.s}
          {T : F^O.Term F^O.S (F^O.type-of F^O.s)} →
  Γ F^O.⊢ t : T →
  F.Term (Γ⇝S Γ) (s⇝s F^O.s)
⊢t⇝t (⊢‘o o:τ∈Γ) = ‘ o:τ∈Γ⇝x o:τ∈Γ
⊢t⇝t (⊢ƛ ⊢e) = λ‘x→ (⊢t⇝t ⊢e)
⊢t⇝t (⊢⊘ ⊢e o:τ∈Γ) = ⊢t⇝t ⊢e · ‘ o:τ∈Γ⇝x o:τ∈Γ
⊢t⇝t (⊢decl ⊢e) = let‘x= tt ‘in ⊢t⇝t ⊢e
⊢t⇝t (⊢inst ⊢e2 ⊢e1) = let‘x= ⊢t⇝t ⊢e2 ‘in ⊢t⇝t ⊢e1
- ...
```

Typed overloaded variables `⊢‘o` carry information about the instance that was resolved for o. We translate the resolved instance to the unique variable in System F using the `o:τ∈Γ⇝x` function from above.
Constraint abstractions translate to normal abstractions.
An implicitly resolved constraint translates to an explicit application that passes the resolved instance as argument. We again use function `o:τ∈Γ⇝x` to translate the resolved instance to the corresponding unique variable.
The `decl` expression could be removed by the translation as seen in the example at the beginning. Instead `decl` expressions are translated to useless let bindings that bind a unit value. Because `decl` expressions bind a new overloaded variable in System $\mathrm{F_O}$, removing them would result in a variable binding less in System F and hence, more complex proofs.
We translate `inst` expressions to `let` expressions that introduce an additional binding not present in System $\mathrm{F_O}$.

5.2 Type Preservation

Terms

We first look at the final proof of type preservation for the Dictionary Passing Transform to motivate all necessary lemmas. Type preservation is proven by induction over the typing rules of System $\mathrm{F_O}$. The function `⊢t⇝⊢t` produces a typed System F term for an arbitrary typed System $\mathrm{F_O}$ term $\vdash t$. The untyped translated System $\mathrm{F_O}$ term `⊢t⇝t` t gets typed in the translated context `Γ⇝Γ` Γ and has the typing result `T⇝T` T, where `T⇝T` is the function that translates untyped types and kinds.

```
⊢t⇝⊢t : {Γ : F^O.Ctx F^O.S} {t : F^O.Term F^O.S F^O.s}
         {T : F^O.Term F^O.S (F^O.type-of F^O.s)} →
  (⊢t : Γ F^O.⊢ t : T) →
  (Γ⇝Γ Γ) F.⊢ (⊢t⇝t ⊢t) : (T⇝T T)
⊢t⇝⊢t (⊢‘x {x = x} Γx≡τ) = ⊢‘x (Γx≡τ⇝Γx≡τ x Γx≡τ)
⊢t⇝⊢t (⊢‘o o:τ∈Γ) = ⊢‘x (o:τ∈Γ⇝Γx≡τ o:τ∈Γ)
⊢t⇝⊢t (⊢let ⊢e2 ⊢e1) = ⊢let (⊢t⇝⊢t ⊢e2)
  (subst (_ F.⊢ ⊢t⇝t ⊢e1 :_) τ⇝wk·τ≡wk·τ⇝τ (⊢t⇝⊢t ⊢e1))
⊢t⇝⊢t (⊢ƛ {c = (‘ o : τ)} ⊢e) = ⊢λ
  (subst (_ F.⊢ ⊢t⇝t ⊢e :_) τ⇝wk-inst·τ≡wk·τ⇝τ (⊢t⇝⊢t ⊢e))
```

```
⊢t⇝⊢t (⊢⊘ ⊢e o:τ∈Γ) = ⊢· (⊢t⇝⊢t ⊢e) (⊢‘x (o:τ∈Γ⇝Γx≡τ o:τ∈Γ))
⊢t⇝⊢t (⊢• {τ = τ} {τ’ = τ’} ⊢e) = subst (_ F.⊢ ⊢t⇝t ⊢e • τ⇝τ τ’ :_)
  (τ'⇝τ'[τ⇝τ]≡τ'[τ]⇝τ τ’ τ) (⊢• (⊢t⇝⊢t ⊢e))
- ...
```

Proof $\Gamma x{\equiv}\tau$ that a variable x has type τ in Γ translates to proof that x⇝x x has type τ⇝τ τ in Γ⇝Γ Γ using lemma Γx≡τ⇝Γx≡τ. With the lemma Γx≡τ⇝Γx≡τ the typing rule ⊢‘x can be translated to the typing rule for variables in System F.
Similarly, the lemma o:τ∈Γ⇝Γx≡τ translates the proof that an instance o : τ was resolved for an overloaded variable o to proof that the unique variable o:τ∈Γ⇝x o:τ∈Γ has type τ⇝τ τ in Γ⇝Γ Γ. Using lemma o:τ∈Γ⇝Γx≡τ the typing rule for overloaded variables ⊢‘o can be translated to the typing rule for normal variables ⊢‘x.
Typed let bindings ⊢let $\vdash e_2$ $\vdash e_1$ translate to typed let bindings in System F. The typing rule $\vdash e_2$ is translated directly using the induction hypothesis. Because the typing for e_1 results in wk τ’, proof is needed that τ’ weakened in System $\mathrm{F_O}$ and translated to System F is equivalent to the weakening of the translated τ’ in System F. Lemma τ⇝wk·τ≡wk·τ⇝τ is used to substitute the required equivalence into the translated typing rule ⊢t⇝⊢t $\vdash e_1$.
Typed constraint abstractions ⊢λ translate to normal abstractions in System F. Inside the typing $\vdash e$, the result type τ for e does not need to be weakened because the constraint abstraction only introduced a constraint to context Γ and no actual binding. After the translation the former constraint will be bound by a binding and thus a new item in Γ⇝Γ Γ will exist. To ignore the binding τ is weakened in the abstraction rule ⊢λ. Lemma τ⇝wk-inst·τ≡wk·τ⇝τ proves that translating τ in Γ extended by a constraint is equivalent to weakening τ after the translation. The lemma follows because the constraint translates to an actual binding and consequently, both sides have an additional unnecessary expression binding that τ cannot use.
Implicitly resolved constraints ⊢⊘ carry the information about the instance that was resolved. In System F the former constraint is explicitly passed as variable pointing to the correct translated instance. Thus, ⊢⊘ results in typed application ⊢·. We apply the correct instance using lemma o:τ∈Γ⇝Γx≡τ to get the correct unique variable for the resolved constraint.
The Type application rule ⊢• contains type in type substitution. Hence, we need proof that it is irrelevant, if τ’ is substituted into τ and then translated or both τ and τ’ are translated and substituted in System F. Using lemma τ'⇝τ'[τ⇝τ]≡τ'[τ]⇝τ we can substitute the equivalence into the System F typing rule ⊢• (⊢t⇝⊢t$\vdash e$).
The translation of ⊢⊤, ⊢λ, ⊢·, ⊢decl and ⊢inst is either a direct translation or uses similar ideas and no other lemmas than the ones discussed.

Renaming

Both τ⇝wk·τ≡wk·τ⇝τ and τ⇝wk-inst·τ≡wk·τ⇝τ directly follow from a more general lemma ⊢ρ⇝ρ·τ⇝τ≡ρτ⇝τ for arbitrary renamings. The lemma ⊢ρ⇝ρ·τ⇝τ≡ρτ⇝τ proves that translating both the typed renaming $\vdash\rho$ and type τ and then applying the renaming in System F is equivalent to applying the renaming ρ in System $\mathrm{F_O}$ and then translating renamed τ. The lemma can be proven by induction over System $\mathrm{F_O}$ types τ.

```
⊢ρ⇝ρ·τ⇝τ≡ρτ⇝τ : {ρ : F^O.Ren F^O.S₁ F^O.S₂}
                {Γ₁ : F^O.Ctx F^O.S₁} {Γ₂ : F^O.Ctx F^O.S₂} →
```

```
  (⊢ρ : ρ FO.: Γ1 ⇒r Γ2) →
  (τ : FO.Type FO.S1) →
  F.ren (⊢ρ⇝ρ ⊢ρ) (τ⇝τ τ) ≡ τ⇝τ (FO.ren ρ τ)
⊢ρ⇝ρ·τ⇝τ≡ρτ⇝τ ⊢ρ (‘ x) = cong ‘_ (⊢ρ⇝ρ·x⇝x≡ρx⇝x ⊢ρ x)
⊢ρ⇝ρ·τ⇝τ≡ρτ⇝τ ⊢ρ ([ ‘ o : τ ]⇒ τ’) = cong2 _⇒_
  (⊢ρ⇝ρ·τ⇝τ≡ρτ⇝τ ⊢ρ τ) (⊢ρ⇝ρ·τ⇝τ≡ρτ⇝τ ⊢ρ τ’)
- ...
```

The case for type variables needs an additional lemma `⊢ρ⇝ρ·x⇝x≡ρx⇝x` specifically for type variables. Lemma `⊢ρ⇝ρ·x⇝x≡ρx⇝x` proves an analogous statement, but for type variables applied to a renaming: `(⊢ρ⇝ρ ⊢ρ) (x⇝x x) ≡ x⇝x (ρ x)`. This statement can be proven via straight forward induction over typed System F_O renamings $\vdash\rho$.
All other cases follow directly from the induction hypothesis. The only small exception is the constraint type, where we need to respect that it translates to a function type.

Substitution

Similar to renamings, the lemma for single substitution on types `τ'⇝τ'[τ⇝τ]≡τ'[τ]⇝τ` follows from a more general lemma about type in type substitutions: `τ'⇝τ'[τ⇝τ]≡τ'[τ]⇝τ τ τ’ = ⊢σ⇝σ·τ⇝τ≡στ⇝τ FO.⊢single-types τ’`. The more general lemma `⊢σ⇝σ·τ⇝τ≡στ⇝τ` follows by straight forward induction over System F_O types as well, except the case for type variables. Other than with renamings, the cases for lemma `⊢σ⇝σ·x⇝x≡σx⇝τ` do not follow directly from the induction hypothesis. To understand why, we at look at the case `⊢exts`.

```
⊢σ⇝σ·x⇝x≡σx⇝τ : {σ : FO.Sub FO.S1 FO.S2}
                {Γ1 : FO.Ctx FO.S1} {Γ2 : FO.Ctx FO.S2} →
  (⊢σ : σ FO.: Γ1 ⇒s Γ2) →
  (x : FO.Var FO.S1 τs) →
  F.sub (⊢σ⇝σ ⊢σ) (‘ x⇝x x) ≡ τ⇝τ (FO.sub σ (‘ x))
⊢σ⇝σ·x⇝x≡σx⇝τ (⊢exts ⊢σ) (here refl) = refl
⊢σ⇝σ·x⇝x≡σx⇝τ (⊢exts {σ = σ} ⊢σ) (there x) = trans
  (cong F.wk (⊢σ⇝σ·x⇝x≡σx⇝τ ⊢σ x)) (⊢ρ⇝ρ·τ⇝τ≡ρτ⇝τ FO.⊢wkr (σ x))
```

The case `⊢exts` is proven via induction over variable x, similar to how `exts` is defined. The base case holds by definition. In the induction case we weaken both sides of the equality that results from the outer induction hypothesis. We then combine the weakened induction hypothesis with proof that weakenings preserve the translation using transitivity. The intuition here is that we need the renaming lemma `⊢ρ⇝ρ·τ⇝τ≡ρτ⇝τ` because `exts` is defined by weakening the term that result of the substitution σ being applied to the variable x.
Both `⊢ids` and `⊢types` follow directly from the induction hypothesis. The cases for `⊢drops`, `⊢drop-cstrs` and `⊢ext-cstrs` are similar to `⊢exts`.

Variables

We first look at the proof for lemma `Γx≡τ⇝Γx≡τ`. Lemma `Γx≡τ⇝Γx≡τ` is proven via induction over the System F_O context Γ.

```
Γx≡τ⇝Γx≡τ : ∀ {Γ : F^O.Ctx F^O.S} {τ : F^O.Type F^O.S} (x : F^O.Var F^O.S e_s) →
  F^O.lookup Γ x ≡ τ →
  F.lookup (Γ⇝Γ Γ) (x⇝x x) ≡ (τ⇝τ τ)
Γx≡τ⇝Γx≡τ {Γ = Γ ▶ τ} (here refl) refl = ⊢ρ⇝ρ·τ⇝τ≡ρτ⇝τ F^O.⊢wk_r τ
Γx≡τ⇝Γx≡τ {Γ = Γ ▶ _} {τ'} (there x) refl = trans
  (cong F.wk (Γx≡τ⇝Γx≡τ x refl))
  (⊢ρ⇝ρ·τ⇝τ≡ρτ⇝τ F^O.⊢wk_r (F^O.lookup Γ x))
- ...
```

As an example we will look at case Γ ▶ τ. The case is proven via induction over variables x. The prove follows the same reasoning as the $\vdash\mathsf{ext}_s$ case for substitutions above. Because the function lookup weakens the type τ that is looked up in Γ in both the base case and induction step, both use lemma ⊢ρ⇝ρ·τ⇝τ≡ρτ⇝τ to account for the weakening.

The case Γ ▸ c is a little more complicated but uses similar concepts. Additional complexity arises because we need to deal with the fact that constraints were ignored by the lookup method in System F_O but then are translated to actual context items in System F.

Lemma o:τ∈Γ⇝Γx≡τ can proven via induction over the type for resolved constraints [c]∈ Γ. The proof is analogous to the proof shown for Γx≡τ⇝Γx≡τ because the type for resolved constraints preserves the structure of context Γ.

This finishes up the type preservation proof for the Dictionary Passing Transform from System F_O to System F.

6 Further Work and Conclusion

6.1 Hindley Milner with Overloading

In this scenario the source language for the Dictionary Passing Transform would be an extended Hindley-Milner [7] based system HM_O and the target language would be Hindley-Milner. The Hindley-Milner system is a restricted form of System F. Formalizing Hindley-Milner would require two new sorts, m_s and p_s for mono and poly types, in favour of the sort for arbitrary types τ_s. Poly types can include quantification over type variables while mono types consist only of primitive types and type variables. Usually all language constructs are restricted to mono types, except let bound variables. Hence polymorphism in Hindley-Milner is also called let polymorphism. As a result, constraints must have the form $o : m$, where m is a mono type. Because there are no expression level constructs to introduce type variables in Hindley-Milner, we would need to embed constraints into explicit type annotation of instances instead of introducing them on the expression level. The explicit type annotation for instances would allow poly types because instance expressions translate to let bindings after all. But instances would need to be restricted as well. For each overloaded variable o, all instances would need to differ in the type of their first argument. With these two restrictions full type inference for instances and overloaded variables should be preserved. The inference algorithm would treat instance expressions similar to let bindings and could infer the type of an overloaded identifier via the type of the first argument applied. For now it remains unclear if constraints still could be eliminated deterministically by the inference algorithm.

6.2 Proving Semantic Preservation

For now System F_O does not have semantics formalized. Semantics for System F_O would need to be typed semantics because applications ` o · e_1 .. · e_n need type information to reduce properly. The correct instance for o needs to be resolved based on the types of arguments e_1 .. e_n. More specifically, to formalize small step semantics we would need to apply the restriction mentioned above and restrict all instances for an overloaded variable o to differ in the type of their first argument. In consequence, the resolved instance for o in a single application step ` o · e would be decidable. Let ⊢e ↪ ⊢e' be such a typed small step semantic for System F_O. We would need to prove something similar to: If ⊢e ↪ ⊢e' then ∃ [e”] (⊢e↪e'⇝e↪e' ⊢e ↪* e”) × (⊢e↪e'⇝e↪e' ⊢e' ↪* e”), where ⊢e↪e'⇝e↪e' translates typed System F_O reductions to a untyped System F reductions. Instead of translating reduction steps directly, we prove that both translated ⊢e and ⊢e' reduce to a System F expression e” using finite many reduction steps. This more general formulation is needed because there might be more reduction steps in the translated System F expression than in the System F_O expression. For example, an implicitly resolved constraint in System F_O needs to be explicitly passed using an additional application step in System F. For now it remains unclear if semantic preservation can be proven using induction over the typed semantic rules or if logical relations are needed [1].

6.3 Related Work

The ideas for the required restrictions to preserve the inference algorithm in Section 6.1 originate from System O [8]. System O is a language extension to the Hindley-Milner System. In contrast to System F_O, constraints are not introduced on the expression level and instead are introduced via explicit type annotations of instances as part of forall types. For instance, the valid System F_O type `∀α. ∀β. [a : α → α → α] => [b : β → β → β] => ..` would be expressed as `∀α. (a : α → α → α) => ∀β. (b : β → β → β) => ..` in System O. Here we only introduce one constraint per type variable, but a list of constraints is allowed. Originally the plan was to formalize System O in Agda, but multiple issues arose in the type preservation proof. First, because we have a list of n constraints for each forall type, translating them results in n new lambda bindings in one induction step. Furthermore, the translation of the System O type above must pull out quantifiers, because translating the constraints directly to higher oder functions would break the rule that function types are only allowed to be built from mono types. Thus the translated System O type should not be `∀α. (α → α → α) → ∀β. (β → β → β) → ..` but rather `∀α. ∀β. (α → α → α) → (β → β → β) → ...` Including the additional transform on types complicates the type preservation proof immensely, because the transform affects the type of the next n expressions and thus straight forward induction cannot be used.
There exist other formalizations that are more similar to actual typeclasses in Haskell [9] [4]. A more general approach to constraint types is presented by the theory of qualified types [5].

6.4 Conclusion

We have formalized both System F and System F_O in Agda. System F_O acts as a core calculus that captures the essence of overloading. Using Agda we formalized the Dictionary Passing Transform between System F and System F_O. We proved the System

F formalization to be sound and the Dictionary Passing Transform from System F_O to System F to be type preserving. The full formalization of System F, System F_O and the Dictionary Passing Transform can be found as Agda code files [2]. A reasonable next step would be to prove semantic preservation for the Dictionary Passing Transform.

[2] Formalizations and proofs as Agda code files: `https://github.com/Mari-W/System-Fo/tree/main/proofs`

References

1. Abel, A., Allais, G., Hameer, A., Pientka, B., Momigliano, A., Schäfer, S. & Stark, K. POPLMark reloaded: Mechanizing proofs by logical relations. *Journal Of Functional Programming.* **29** pp. e19 (2019), http://dx.doi.org/10.1017/S0956796819000170
2. Barendregt, H. Introduction to generalized type systems. *Journal Of Functional Programming.* **1**, 125-154 (1991), https://doi.org/10.1017%2Fs0956796800020025
3. Bove, A., Dybjer, P., Norell, U. (2009). A Brief Overview of Agda – A Functional Language with Dependent Types. In: Berghofer, S., Nipkow, T., Urban, C., Wenzel, M. (eds) Theorem Proving in Higher Order Logics. TPHOLs 2009. Lecture Notes in Computer Science, vol 5674. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-03359-9_6
4. Cordelia V. Hall, Kevin Hammond, Simon L. Peyton Jones, and Philip L. Wadler. 1996. Type classes in Haskell. ACM Trans. Program. Lang. Syst. 18, 2 (March 1996), 109–138. https://doi.org/10.1145/227699.227700
5. Jones, M.P. (1992). A theory of qualified types. In: Krieg-Brückner, B. (eds) ESOP '92. ESOP 1992. Lecture Notes in Computer Science, vol 582. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-55253-7_17
6. Martin-Löf, P. & Sambin, G. Intuitionistic Type Theory. (Bibliopolis, 1984), https://www.cse.chalmers.se/~peterd/papers/MartinL%C3%B6f1984.pdf
7. Milner, R. A theory of type polymorphism in programming. *Journal Of Computer And System Sciences.* **17**, 348-375 (1978), https://www.sciencedirect.com/science/article/pii/0022000078900144
8. Odersky, M., Wadler, P. & Wehr, M. A Second Look at Overloading. *Proceedings Of The Seventh International Conference On Functional Programming Languages And Computer Architecture.* pp. 135-146 (1995), https://doi.org/10.1145/224164.224195
9. P. Wadler and S. Blott. 1989. How to make ad-hoc polymorphism less ad hoc. In Proceedings of the 16th ACM SIGPLAN-SIGACT symposium on Principles of programming languages (POPL '89). Association for Computing Machinery, New York, NY, USA, 60–76. https://doi.org/10.1145/75277.75283

Declaration

I hereby declare, that I am the sole author and composer of my thesis and that no other sources or learning aids, other than those listed, have been used. Furthermore, I declare that I have acknowledged the work of others by providing detailed references of said work.
I also hereby declare that my thesis has not been prepared for another examination or assignment, either in its entirety or excerpts thereof.

Place, Date

Signature