

# Formal Methods

## Lecture 10

(B. Pierce's slides for the book “Types and Programming Languages”)

# Subtyping

## Motivation

---

With our usual typing rule for applications

$$\frac{\Gamma \vdash t_1 : T_{11} \rightarrow T_{12} \quad \Gamma \vdash t_2 : T_{11}}{\Gamma \vdash t_1 \ t_2 : T_{12}} \quad (\text{T-App})$$

the term

$(\lambda r:\{x:\text{Nat}\}. \ r.x) \ \{x=0,y=1\}$

is *not* well typed.

## Motivation

---

With our usual typing rule for applications

$$\frac{\Gamma \vdash t_1 : T_{11} \rightarrow T_{12} \quad \Gamma \vdash t_2 : T_{11}}{\Gamma \vdash t_1 \ t_2 : T_{12}} \quad (\text{T-App})$$

the term

$(\lambda r:\{x:\text{Nat}\}. \ r.x) \ \{x=0,y=1\}$

is *not* well typed.

But this is silly: all we're doing is passing the function a *better* argument than it needs.

# Polymorphism

---

A *polymorphic* function may be applied to many different types of data.

Varieties of polymorphism:

- △ Parametric polymorphism (ML-style)
- △ Subtype polymorphism (OO-style)
- △ Ad-hoc polymorphism (overloading)

Our topic for the next few lectures is *subtype* polymorphism, which is based on the idea of *subsumption*.

## Subsumption

---

More generally: some *types* are better than others, in the sense that a value of one can always safely be used where a value of the other is expected.

We can formalize this intuition by introducing

1. a *subtyping* relation between types, written  $S <: T$
2. a rule of *subsumption* stating that, if  $S <: T$ , then any value of type  $S$  can also be regarded as having type  $T$

$$\frac{\Gamma \vdash t : S \quad S <: T}{\Gamma \vdash t : T} \quad (\text{T-Sub})$$

## Example

---

We will define subtyping between record types so that, for example,

$$\{x:\text{Nat}, y:\text{Nat}\} <: \{x:\text{Nat}\}$$

So, by subsumption,

$$\vdash \{x=0, y=1\} : \{x:\text{Nat}\}$$

and hence

$$(\lambda r:\{x:\text{Nat}\}. r.x) \{x=0, y=1\}$$

is well typed.

## The Subtype Relation: Records

---

“Width subtyping” (forgetting fields on the right):

$$\{l_i : T_i \mid i \in 1 \dots n+k\} <: \{l_i : T_i \mid i \in 1 \dots n\} \quad (\text{S-RecdWidth})$$

Intuition:  $\{x:\text{Nat}\}$  is the type of all records with *at least* a numeric  $x$  field.

Note that the record type with *more* fields is a *subtype* of the record type with fewer fields.

Reason: the type with more fields places a *stronger constraint* on values, so it describes *fewer values*.



## The Subtype Relation: Records

---

Permutation of fields:

$$\frac{\{k_j : S_j \mid j \in 1..n\} \text{ is a permutation of } \{l_i : T_i \mid i \in 1..n\}}{\{k_j : S_j \mid j \in 1..n\} <: \{l_i : T_i \mid i \in 1..n\}} \quad (\text{S-RcdPer m})$$

By using S-RcdPer m together with S-RcdWidth and S-Trans allows us to drop arbitrary fields within records.

## The Subtype Relation: Records

---

“Depth subtyping” within fields:

$$\frac{\text{for each } i \quad S_i <: T_i}{\{ l_i : S_i \mid i \in 1 \dots n \} <: \{ l_i : T_i \mid i \in 1 \dots n \}} \quad (\text{S-RcdDepth})$$

The types of individual fields may change.

## Example

---

$$\frac{}{\{a:\text{Nat}, b:\text{Nat}\} <: \{a:\text{Nat}\}} \text{S-RcdWidth h}$$
$$\frac{}{\{m:\text{Nat}\} <: \{ \}} \text{S-RcdWidth h}$$
$$\frac{}{\{x:\{a:\text{Nat}, b:\text{Nat}\}, y:\{m:\text{Nat}\}\} <: \{x:\{a:\text{Nat}\}, y:\{ \}\}} \text{S-RcdDepth h}$$

## Variations

---

Real languages often choose not to adopt all of these record subtyping rules. For example, in Java,

- ▲ A subclass may not change the argument or result types of a method of its superclass (i.e., no depth subtyping)
- ▲ Each class has just one superclass (“single inheritance” of classes)
  - *each class member (field or method) can be assigned a single index, adding new indices “on the right” as more members are added in subclasses (i.e., no permutation for classes)*
- ▲ A class may implement multiple *interfaces* (“multiple inheritance” of interfaces)  
I.e., permutation is allowed for interfaces.

## The Subtype Relation: Arrow types

---

$$\frac{T_1 <: S_1 \quad S_2 <: T_2}{S_1 \rightarrow S_2 <: T_1 \rightarrow T_2} \quad (\text{S-Arrow})$$

Note the order of  $T_1$  and  $S_1$  in the first premise. The subtype relation is *contravariant* in the left-hand sides of arrows and *covariant* in the right-hand sides.

Intuition: if we have a function  $f$  of type  $S_1 \rightarrow S_2$ , then we know that  $f$  accepts elements of type  $S_1$ ; clearly,  $f$  will also accept elements of any subtype  $T_1$  of  $S_1$ . The type of  $f$  also tells us that it returns elements of type  $S_2$ ; we can also view these results belonging to any supertype  $T_2$  of  $S_2$ . That is, any function  $f$  of type  $S_1 \rightarrow S_2$  can also be viewed as having type  $T_1 \rightarrow T_2$ .

## The Subtype Relation: Top

---

It is convenient to have a type that is a supertype of every type. We introduce a new type constant `Top`, plus a rule that makes `Top` a maximum element of the subtype relation.

$$S <: \text{Top} \qquad (\text{S-Top})$$

Cf. `Object` in Java.

## The Subtype Relation: General rules

---

$S <: S$  (S-Ref1)

$$\frac{S <: U \quad U <: T}{S <: T}$$
 (S-Trans)

# Subtype relation

---

$$S <: S \quad (\text{S-REFL})$$

$$\frac{S <: U \quad U <: T}{S <: T} \quad (\text{S-TRANS})$$

$$\{l_i : T_i \mid i \in 1..n+k\} <: \{l_i : T_i \mid i \in 1..n\} \quad (\text{S-RCDWIDTH})$$

$$\frac{\text{for each } i \quad S_i <: T_i}{\{l_i : S_i \mid i \in 1..n\} <: \{l_i : T_i \mid i \in 1..n\}} \quad (\text{S-RCDDEPTH})$$

$$\frac{\{k_j : S_j \mid j \in 1..n\} \text{ is a permutation of } \{l_i : T_i \mid i \in 1..n\}}{\{k_j : S_j \mid j \in 1..n\} <: \{l_i : T_i \mid i \in 1..n\}} \quad (\text{S-RCDPERM})$$

$$\frac{T_1 <: S_1 \quad S_2 <: T_2}{S_1 \rightarrow S_2 <: T_1 \rightarrow T_2} \quad (\text{S-ARROW})$$

$$S <: \text{Top} \quad (\text{S-TOP})$$



# Properties of Subtyping

## Safety

---

*Statements* of progress and preservation theorems are unchanged from  $\lambda \rightarrow$ .

*Proofs* become a bit more involved, because the typing relation is no longer *syntax directed*.

Given a derivation, we don't always know what rule was used in the last step. The rule T-Sub could appear anywhere.

$$\frac{\Gamma \vdash t : S \quad S <: T}{\Gamma \vdash t : T} \quad (\text{T-Sub})$$

## Preservation

---

*Theorem:* If  $\Gamma \vdash t : T$  and  $t \rightarrow t'$ , then  $\Gamma \vdash t' : T$ .

*Proof:* By induction on typing derivations.

(Which cases are likely to be hard?)

## Subsumption case

---

*Case* T-Sub:  $t : S \quad S \leq T$

By the induction hypothesis,  $\Gamma \vdash t' : S$ . By T-Sub,  $\Gamma \vdash t : T$ .

Not hard!

## Application case

---

*Case* T-App:

$$t = t_1 \ t_2 \quad \Gamma \vdash t_1 : T_{11} \rightarrow T_{12} \quad \Gamma \vdash t_2 : T_{11} \quad T = T_{12}$$

By the inversion lemma for evaluation, there are three rules by which  $t \rightarrow t'$  can be derived: E-App1, E-App2, and E-AppAbs. Proceed by cases.

## Application case

---

*Case* T-App:

$$t = t_1 \ t_2 \quad \Gamma \vdash t_1 : T_{11} \rightarrow T_{12} \quad \Gamma \vdash t_2 : T_{11} \quad T = T_{12}$$

By the inversion lemma for evaluation, there are three rules by which  $t \rightarrow t'$  can be derived: E-App1, E-App2, and E-AppAbs. Proceed by cases.

*Subcase* E-App1:  $t_1 \rightarrow t'_1 \quad t' = t'_1 \ t_2$

The result follows from the induction hypothesis and T-App.

$$\frac{\Gamma \vdash t_1 : T_{11} \rightarrow T_{12} \quad \Gamma \vdash t_2 : T_{11}}{\Gamma \vdash t_1 \ t_2 : T_{12}} \quad (\text{T-App})$$

## Application case

---

*Case* T-App:

$$t = t_1 \ t_2 \quad \Gamma \vdash t_1 : T_{11} \rightarrow T_{12} \quad \Gamma \vdash t_2 : T_{11} \quad T = T_{12}$$

By the inversion lemma for evaluation, there are three rules by which  $t \rightarrow t'$  can be derived: E-App1, E-App2, and E-AppAbs. Proceed by cases.

*Subcase* E-App1:  $t_1 \rightarrow t'_1 \quad t' = t'_1 \ t_2$

The result follows from the induction hypothesis and T-App.

$$\frac{\Gamma \vdash t_1 : T_{11} \rightarrow T_{12} \quad \Gamma \vdash t_2 : T_{11}}{\Gamma \vdash t_1 \ t_2 : T_{12}} \quad (\text{T-App})$$

$$\frac{t_1 \rightarrow t'_1}{t_1 \ t_2 \rightarrow t'_1 \ t_2} \quad (\text{E-App1})$$

**Case** T-App (continued):

$$t = t_1 \ t_2 \quad \Gamma \vdash t_1 : T_{11} \rightarrow T_{12} \quad \Gamma \vdash t_2 : T_{11} \quad T = T_{12}$$

**Subcase** E-App2:  $t_1 = v_1 \quad t_2 \rightarrow t'_2 \quad t' = v_1 \ t'_2$

Similar.

$$\frac{\Gamma \vdash t_1 : T_{11} \rightarrow T_{12} \quad \Gamma \vdash t_2 : T_{11}}{\Gamma \vdash t_1 \ t_2 : T_{12}} \quad (\text{T-App})$$

$$\frac{t_2 \rightarrow t'_2}{v_1 \ t_2 \rightarrow v_1 \ t'_2} \quad (\text{E-App2})$$



Case T-APP (CONTINUED):

$$t = t_1 \ t_2 \quad \Gamma \vdash t_1 : T_{11} \rightarrow T_{12} \quad \Gamma \vdash t_2 : T_{11} \quad T = T_{12}$$

Subcase E-APPABS:

$$t_1 = \lambda x:S_{11}. \ t_{12} \quad t_2 = v_2 \quad t' = [x \mapsto v_2]t_{12}$$

By the inversion lemma for the typing relation...  $T_{11} <: S_{11}$  and  $\Gamma, x:S_{11} \vdash t_{12} : T_{12}$ .

Case T-APP (CONTINUED):

$$t = t_1 \ t_2 \quad \Gamma \vdash t_1 : T_{11} \rightarrow T_{12} \quad \Gamma \vdash t_2 : T_{11} \quad T = T_{12}$$

Subcase E-APPAbs:

$$t_1 = \lambda x:S_{11}. \ t_{12} \quad t_2 = v_2 \quad t' = [x \mapsto v_2]t_{12}$$

By the inversion lemma for the typing relation...  $T_{11} <: S_{11}$  and  $\Gamma, x:S_{11} \vdash t_{12} : T_{12}$ .

By T-SUB,  $\Gamma \vdash t_2 : S_{11}$ .

By the substitution lemma,  $\Gamma \vdash t' : T_{12}$ , and we are done.

$$\frac{\Gamma \vdash t_1 : T_{11} \rightarrow T_{12} \quad \Gamma \vdash t_2 : T_{11}}{\Gamma \vdash t_1 \ t_2 : T_{12}} \quad (\text{T-APP})$$

$$(\lambda x:T_{11}. t_{12}) \ v_2 \longrightarrow [x \mapsto v_2]t_{12} \quad (\text{E-APPAbs})$$

## Inversion Lemma for Typing

---

*Lemma:* If  $\Gamma \vdash \lambda x:S_1. s_2 : T_1 \rightarrow T_2$ , then  $T_1 <: S_1$  and  $\Gamma, x:S_1 \vdash s_2 : T_2$ .

*Proof:* Induction on typing derivations.

## Inversion Lemma for Typing

---

*Lemma:* If  $\Gamma \vdash \lambda x:S_1. s_2 : T_1 \rightarrow T_2$ , then  $T_1 <: S_1$  and  $\Gamma, x:S_1 \vdash s_2 : T_2$ .

*Proof:* Induction on typing derivations.

*Case T-Sub:*  $\lambda x:S_1. s_2 : U \quad U <: T_1 \rightarrow T_2$

## Inversion Lemma for Typing

---

*Lemma:* If  $\Gamma \vdash \lambda x:S_1.s_2 : T_1 \rightarrow T_2$ , then  $T_1 <: S_1$  and  $\Gamma, x:S_1 \vdash s_2 : T_2$ .

*Proof:* Induction on typing derivations.

*Case T-Sub:*  $\lambda x:S_1.s_2 : U \quad U <: T_1 \rightarrow T_2$

We want to say “By the induction hypothesis...”, but the IH does not apply (we do not know that  $U$  is an arrow type).

## Inversion Lemma for Typing

---

*Lemma:* If  $\Gamma \vdash \lambda x:S_1. s_2 : T_1 \rightarrow T_2$ , then  $T_1 <: S_1$  and  $\Gamma, x:S_1 \vdash s_2 : T_2$ .

*Proof:* Induction on typing derivations.

*Case T-Sub:*  $\lambda x:S_1. s_2 : U \quad U <: T_1 \rightarrow T_2$

We want to say “By the induction hypothesis...”, but the IH does not apply (we do not know that  $U$  is an arrow type). Need another lemma...

*Lemma:* If  $U <: T_1 \rightarrow T_2$ , then  $U$  has the form  $U_1 \rightarrow U_2$ , with  $T_1 <: U_1$  and  $U_2 <: T_2$ . (Proof: by induction on subtyping derivations.)

## Inversion Lemma for Typing

---

*Lemma:* If  $\Gamma \vdash \lambda x:S_1. s_2 : T_1 \rightarrow T_2$ , then  $T_1 <: S_1$  and  $\Gamma, x:S_1 \vdash s_2 : T_2$ .

*Proof:* Induction on typing derivations.

*Case T-Sub:*  $\lambda x:S_1. s_2 : U \quad U <: T_1 \rightarrow T_2$

We want to say “By the induction hypothesis...”, but the IH does not apply (we do not know that  $U$  is an arrow type). Need another lemma...

*Lemma:* If  $U <: T_1 \rightarrow T_2$ , then  $U$  has the form  $U_1 \rightarrow U_2$ , with  $T_1 <: U_1$  and  $U_2 <: T_2$ . (Proof: by induction on subtyping derivations.)

By this lemma, we know  $U = U_1 \rightarrow U_2$ , with  $T_1 <: U_1$  and  $U_2 <: T_2$ .

## Inversion Lemma for Typing

---

*Lemma:* If  $\Gamma \vdash \lambda x:S_1. s_2 : T_1 \rightarrow T_2$ , then  $T_1 <: S_1$  and  $\Gamma, x:S_1 \vdash s_2 : T_2$ .

*Proof:* Induction on typing derivations.

*Case T-Sub:*  $\lambda x:S_1. s_2 : U \quad U <: T_1 \rightarrow T_2$

We want to say “By the induction hypothesis...”, but the IH does not apply (we do not know that  $U$  is an arrow type). Need another lemma...

*Lemma:* If  $U <: T_1 \rightarrow T_2$ , then  $U$  has the form  $U_1 \rightarrow U_2$ , with  $T_1 <: U_1$  and  $U_2 <: T_2$ . (Proof: by induction on subtyping derivations.)

By this lemma, we know  $U = U_1 \rightarrow U_2$ , with  $T_1 <: U_1$  and  $U_2 <: T_2$ . The IH now applies, yielding  $U_1 <: S_1$  and  $\Gamma, x:S_1 \vdash s_2 : U_2$ .



## Inversion Lemma for Typing

---

*Lemma:* If  $\Gamma \vdash \lambda x:S_1. s_2 : T_1 \rightarrow T_2$ , then  $T_1 <: S_1$  and  $\Gamma, x:S_1 \vdash s_2 : T_2$ .

*Proof:* Induction on typing derivations.

*Case T-Sub:*  $\lambda x:S_1. s_2 : U \quad U <: T_1 \rightarrow T_2$

We want to say “By the induction hypothesis...”, but the IH does not apply (we do not know that  $U$  is an arrow type). Need another lemma...

*Lemma:* If  $U <: T_1 \rightarrow T_2$ , then  $U$  has the form  $U_1 \rightarrow U_2$ , with  $T_1 <: U_1$  and  $U_2 <: T_2$ . (Proof: by induction on subtyping derivations.)

By this lemma, we know  $U = U_1 \rightarrow U_2$ , with  $T_1 <: U_1$  and  $U_2 <: T_2$ . The IH now applies, yielding  $U_1 <: S_1$  and  $\Gamma, x:S_1 \vdash s_2 : U_2$ . From  $U_1 <: S_1$  and  $T_1 <: U_1$ , rule S-Trans gives  $T_1 <: S_1$ .

## Inversion Lemma for Typing

---

*Lemma:* If  $\Gamma \vdash \lambda x:S_1. s_2 : T_1 \rightarrow T_2$ , then  $T_1 <: S_1$  and  $\Gamma, x:S_1 \vdash s_2 : T_2$ .

*Proof:* Induction on typing derivations.

*Case T-Sub:*  $\lambda x:S_1. s_2 : U \quad U <: T_1 \rightarrow T_2$

We want to say “By the induction hypothesis...”, but the IH does not apply (we do not know that  $U$  is an arrow type). Need another lemma...

*Lemma:* If  $U <: T_1 \rightarrow T_2$ , then  $U$  has the form  $U_1 \rightarrow U_2$ , with  $T_1 <: U_1$  and  $U_2 <: T_2$ . (Proof: by induction on subtyping derivations.)

By this lemma, we know  $U = U_1 \rightarrow U_2$ , with  $T_1 <: U_1$  and  $U_2 <: T_2$ . The IH now applies, yielding  $U_1 <: S_1$  and  $\Gamma, x:S_1 \vdash s_2 : U_2$ . From  $U_1 <: S_1$  and  $T_1 <: U_1$ , rule S-Trans gives  $T_1 <: S_1$ . From  $\Gamma, x:S_1 \vdash s_2 : U_2$  and  $U_2 <: T_2$ , rule T-Sub gives  $\Gamma, x:S_1 \vdash s_2 : T_2$ , and we are done.

# Subtyping with Other Features

## Ascription and Casting

---

Ordinary ascription:

$$\frac{\Gamma \vdash t_1 : T}{\Gamma \vdash t_1 \text{ as } T : T} \quad (\text{T-Ascribe})$$

$$v_1 \text{ as } T \longrightarrow v_1 \quad (\text{E-Ascribe})$$

## Ascription and Casting

---

Ordinary ascription:

$$\frac{\Gamma \vdash t_1 : T}{\Gamma \vdash t_1 \text{ as } T : T} \quad (\text{T-Ascribe})$$

$$v_1 \text{ as } T \rightarrow v_1 \quad (\text{E-Ascribe})$$

Casting (cf. Java):

$$\frac{\Gamma \vdash t_1 : S}{\Gamma \vdash t_1 \text{ as } T : T} \quad (\text{T-Cast})$$

$$\frac{\vdash v_1 : T}{v_1 \text{ as } T \rightarrow v_1} \quad (\text{E-Cast})$$

# Subtyping and Variants

---

$$\langle l_i : T_i \rangle_{i \in 1..n} <: \langle l_i : T_i \rangle_{i \in 1..n+k} \quad (\text{S-VARIANTWIDTH})$$

$$\frac{\text{for each } i \quad S_i <: T_i}{\langle l_i : S_i \rangle_{i \in 1..n} <: \langle l_i : T_i \rangle_{i \in 1..n}} \quad (\text{S-VARIANTDEPTH})$$

$$\frac{\langle k_j : S_j \rangle_{j \in 1..n} \text{ is a permutation of } \langle l_i : T_i \rangle_{i \in 1..n}}{\langle k_j : S_j \rangle_{j \in 1..n} <: \langle l_i : T_i \rangle_{i \in 1..n}} \quad (\text{S-VARIANTPERM})$$

$$\frac{\Gamma \vdash t_1 : T_1}{\Gamma \vdash \langle l_1 = t_1 \rangle : \langle l_1 : T_1 \rangle} \quad (\text{T-VARIANT})$$

## Subtyping and Lists

---

$$\frac{S_1 <: T_1}{\text{List } S_1 <: \text{List } T_1} \quad (\text{S-List})$$

I.e., `List` is a covariant type constructor.

## Subtyping and References

---

$$\frac{S_1 <: T_1 \quad T_1 <: S_1}{\text{Ref } S_1 <: \text{Ref } T_1} \quad (\text{S-Ref})$$

I.e., **Ref** is *not* a covariant (nor a contravariant) type constructor. Why?



## Subtyping and References

---

$$\frac{S_1 <: T_1 \quad T_1 <: S_1}{\text{Ref } S_1 <: \text{Ref } T_1} \quad (\text{S-Ref})$$

I.e., **Ref** is *not* a covariant (nor a contravariant) type constructor. Why?

- △ When a reference is *read*, the context expects a **T<sub>1</sub>**, so if **S<sub>1</sub> <: T<sub>1</sub>** then an **S<sub>1</sub>** is ok.

## Subtyping and References

---

$$\frac{S_1 <: T_1 \quad T_1 <: S_1}{\text{Ref } S_1 <: \text{Ref } T_1} \quad (\text{S-Ref})$$

I.e., **Ref** is *not* a covariant (nor a contravariant) type constructor. Why?

- △ When a reference is *read*, the context expects a  $T_1$ , so if  $S_1 <: T_1$  then an  $S_1$  is ok.
- △ When a reference is *written*, the context provides a  $T_1$  and if the actual type of the reference is **Ref**  $S_1$ , someone else may use the  $T_1$  as an  $S_1$ . So we need  $T_1 <: S_1$ .

## Subtyping and Arrays

---

Similarly..

$$\frac{S_1 <: T_1 \quad T_1 <: S_1}{\text{Array } S_1 <: \text{Array } T_1} \quad (\text{S-Ar r ay})$$

## Subtyping and Arrays

---

Similarly..

$$\frac{S_1 <: T_1 \quad T_1 <: S_1}{\text{Array } S_1 <: \text{Array } T_1} \quad (\text{S-Array})$$

$$\frac{S_1 <: T_1}{\text{Array } S_1 <: \text{Array } T_1} \quad (\text{S-ArrayJava})$$

This is regarded (even by the Java designers) as a mistake in the design.

## References again

---

Observation: a value of type `Ref T` can be used in two different ways: as a *source* for values of type `T` and as a *sink* for values of type `T`.

## References again

---

Observation: a value of type `Ref T` can be used in two different ways: as a *source* for values of type `T` and as a *sink* for values of type `T`.

Idea: Split `Ref T` into three parts:

- △ `Source T`: reference cell with “read cabability”
- △ `Sink T`: reference cell with “write cabability”
- △ `Ref T`: cell with both capabilities

## Modified Typing Rules

---

$$\frac{\Gamma \mid \Sigma \vdash t_1 : \text{Source } T_{11}}{\Gamma \mid \Sigma \vdash !t_1 : T_{11}} \quad (\text{T-Deref})$$

$$\frac{\Gamma \mid \Sigma \vdash t_1 : \text{Sink } T_{11} \quad \Gamma \mid \Sigma \vdash t_2 : T_{11}}{\Gamma \mid \Sigma \vdash t_1 := t_2 : \text{Unit}} \quad (\text{T-Assign})$$

## Subtyping rules

---

$$\frac{S_1 <: T_1}{\text{Source } S_1 <: \text{Source } T_1} \quad (\text{S-Source})$$

$$\frac{T_1 <: S_1}{\text{Sink } S_1 <: \text{Sink } T_1} \quad (\text{S-Sink})$$

$$\text{Ref } T_1 <: \text{Source } T_1 \quad (\text{S-RefSource})$$

$$\text{Ref } T_1 <: \text{Sink } T_1 \quad (\text{S-RefSink})$$



# Algorithmic Subtyping

## Syntax-directed rules

---

In the simply typed lambda-calculus (without subtyping), each rule can be “read from bottom to top” in a straightforward way.

$$\frac{\Gamma \vdash t_1 : T_{11} \rightarrow T_{12} \quad \Gamma \vdash t_2 : T_{11}}{\Gamma \vdash t_1 \ t_2 : T_{12}} \quad (\text{T-App})$$

If we are given some  $\Gamma$  and some  $t$  of the form  $t_1 \ t_2$ , we can try to find a type for  $t$  by

1. finding (recursively) a type for  $t_1$
2. checking that it has the form  $T_{11} \rightarrow T_{12}$
3. finding (recursively) a type for  $t_2$
4. checking that it is the same as  $T_{11}$

Technically, the reason this works is that We can divide the “positions” of the typing relation into *input positions* ( $\Gamma$  and  $t$ ) and *output positions* ( $T$ ).

- For the input positions, all metavariables appearing in the premises also appear in the conclusion (so we can calculate inputs to the “subgoals” from the subexpressions of inputs to the main goal)
- For the output positions, all metavariables appearing in the conclusions also appear in the premises (so we can calculate outputs from the main goal from the outputs of the subgoals)

$$\frac{\Gamma \vdash t_1 : T_{11} \rightarrow T_{12} \quad \Gamma \vdash t_2 : T_{11}}{\Gamma \vdash t_1 \ t_2 : T_{12}} \quad (\text{T-App})$$

## Syntax-directed sets of rules

---

The second important point about the simply typed lambda-calculus is that the *set* of typing rules is syntax-directed, in the sense that, for every “input”  $\Gamma$  and  $t$ , there one rule that can be used to derive typing statements involving  $t$ .

E.g., if  $t$  is an application, then we must proceed by trying to use T-App. If we succeed, then we have found a type (indeed, the unique type) for  $t$ . If it fails, then we know that  $t$  is not typable.

—→ no backtracking!

## Non-syntax-directedness of typing

---

When we extend the system with subtyping, both aspects of syntax-directedness get broken.

1. The set of typing rules now includes *two* rules that can be used to give a type to terms of a given shape (the old one plus T-Sub)

$$\frac{\Gamma \vdash t : S \quad S <: T}{\Gamma \vdash t : T} \quad (\text{T-Sub})$$

2. Worse yet, the new rule T-Sub itself is not syntax directed: the inputs to the left-hand subgoal are exactly the same as the inputs to the main goal!  
(Hence, if we translated the typing rules naively into a typechecking function, the case corresponding to T-Sub would cause divergence.)

## Non-syntax-directedness of subtyping

---

Moreover, the subtyping relation is not syntax directed either.

1. There are *lots* of ways to derive a given subtyping statement.
2. The transitivity rule

$$\frac{S <: U \quad U <: T}{S <: T} \quad (\text{S-Trans})$$

is badly non-syntax-directed: the premises contain a metavariable (in an “input position”) that does not appear at all in the conclusion.

To implement this rule naively, we’d have to *guess* a value for **U**!

## What to do?

---

1. Observation: We don't *need* 1000 ways to prove a given typing or subtyping statement — one is enough.  
→ Think more carefully about the typing and subtyping systems to see where we can get rid of excess flexibility
2. Use the resulting intuitions to formulate new “algorithmic” (i.e., syntax-directed) typing and subtyping relations
3. Prove that the algorithmic relations are “the same as” the original ones in an appropriate sense.