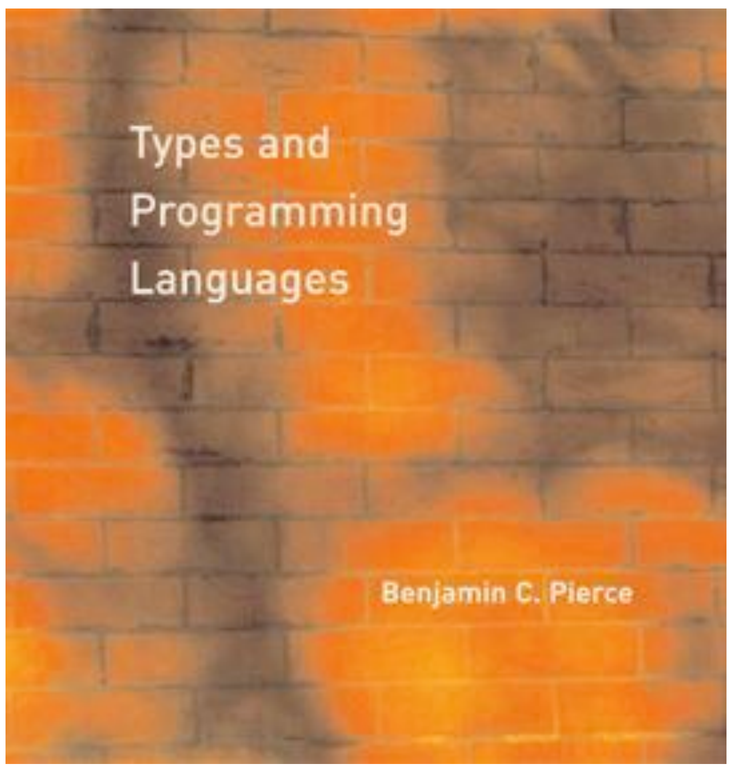
Programming Languages
Fall 2014



Lecture 11: Subtyping

Prof. Liang Huang

huang@qc.cs.cuny.edu

Big Picture

- Part I: Fundamentals
  - Functional Programming and Basic Haskell
  - Proof by Induction and Structural Induction
- Part II: Simply-Typed Lambda-Calculus
  - Untyped Lambda Calculus
  - Simply Typed Lambda Calculus
  - Extensions: Units, Records, Variants
  - References and Memory Allocation
- Part III: Object-Oriented Programming
  - Basic Subtyping
  - Case Study: Featherweight Java

```
class A extends Object { A() { super(); } }
class B extends Object { B() { super(); } }
class Pair extends Object {
    Object fst;
    Object snd;
    // Constructor:
    Pair(Object fst, Object snd) {
        super(); this.fst=fst; this.snd=snd;}
    // Method definition:
    Pair setfst(Object newfst) {
        return new Pair(newfst, this.snd); }}
```

Subtyping

Motivation

With our usual typing rule for applications

$$\frac{\Gamma \vdash \mathtt{t}_1 : \mathtt{T}_{11} \to \mathtt{T}_{12} \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T}_{11}}{\Gamma \vdash \mathtt{t}_1\ \mathtt{t}_2 : \mathtt{T}_{12}} \qquad (\text{T-App})$$

the term

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

is *not* well typed.

Motivation

With our usual typing rule for applications

$$\frac{\Gamma \vdash \mathtt{t}_1 : \mathtt{T}_{11} \rightarrow \mathtt{T}_{12} \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T}_{11}}{\Gamma \vdash \mathtt{t}_1\ \mathtt{t}_2 : \mathtt{T}_{12}} \qquad \text{(T-App)}$$

the term

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

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) C++ templates
- Subtype polymorphism (OO-style) C++ subclass
- Ad-hoc polymorphism (overloading) C++ operator 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 $\mathtt{S} <: \mathtt{T}$
2. a rule of *subsumption* stating that, if $\mathtt{S} <: \mathtt{T}$, then any value of type $\mathtt{S}$ can also be regarded as having type $\mathtt{T}$

$$\frac{\Gamma \vdash \mathtt{t} : \mathtt{S} \qquad \mathtt{S} <: \mathtt{T}}{\Gamma \vdash \mathtt{t} : \mathtt{T}} \qquad \text{(T-SUB)}$$

Example

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

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

So, by subsumption,

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

and hence

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

is well typed.

The Subtype Relation: Records

"Width subtyping" (forgetting fields on the right):

$$\{\mathtt{l}_i\mathtt{:T}_i\ ^{i\in 1..n+k}\} <: \{\mathtt{l}_i\mathtt{:T}_i\ ^{i\in 1..n}\} \quad \text{(S-RcdWidth)}$$

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

Note that the record type with *more* fields is a *sub*type 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:

$$\frac{\{\mathtt{k}_j : \mathtt{S}_j \;^{j \in 1..n}\} \text{ is a permutation of } \{\mathtt{l}_i : \mathtt{T}_i \;^{i \in 1..n}\}}{\{\mathtt{k}_j : \mathtt{S}_j \;^{j \in 1..n}\} <: \{\mathtt{l}_i : \mathtt{T}_i \;^{i \in 1..n}\}} \quad (\text{S-RcdPerm})$$

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

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

The Subtype Relation: Records

"Depth subtyping" within fields:

$$\frac{\text{for each } i \quad \mathtt{S}_i <: \mathtt{T}_i}{\{\mathtt{l}_i\mathtt{:S}_i\ ^{i\in 1..n}\} <: \{\mathtt{l}_i\mathtt{:T}_i\ ^{i\in 1..n}\}} \qquad (\text{S-RcdDepth})$$

The types of individual fields may change.

Example

$$\dfrac{\dfrac{}{\texttt{\{a:Nat,b:Nat\}} <: \texttt{\{a:Nat\}}}\ \textsc{S-RcdWidth} \qquad \dfrac{}{\texttt{\{m:Nat\}} <: \texttt{\{\}}}\ \textsc{S-RcdWidth}}{\texttt{\{x:\{a:Nat,b:Nat\},y:\{m:Nat\}\}} <: \texttt{\{x:\{a:Nat\},y:\{\}\}}}\ \textsc{S-RcdDepth}$$

$$\dfrac{\dfrac{}{\texttt{\{a:Nat,b:Nat\}} <: \texttt{\{a:Nat\}}}\ \textsc{S-RcdWidth} \qquad \dfrac{}{\texttt{\{m:Nat\}} <: \texttt{\{m:Nat\}}}\ \textsc{S-Refl}}{\texttt{\{x:\{a:Nat,b:Nat\},y:\{m:Nat\}\}} <: \texttt{\{x:\{a:Nat\},y:\{m:Nat\}\}}}\ \textsc{S-RcdDepth}$$

$$\dfrac{\dfrac{}{\begin{array}{c}\texttt{\{x:\{a:Nat,b:Nat\},y:\{m:Nat\}\}}\\ <: \texttt{\{x:\{a:Nat,b:Nat\}\}}\end{array}}\ \textsc{S-RcdWidth} \qquad \dfrac{\dfrac{}{\begin{array}{c}\texttt{\{a:Nat,b:Nat\}}\\ <: \texttt{\{a:Nat\}}\end{array}}\ \textsc{S-RcdWidth}}{\begin{array}{c}\texttt{\{x:\{a:Nat,b:Nat\}\}}\\ <: \texttt{\{x:\{a:Nat\}\}}\end{array}}\ \textsc{S-RcdDepth}}{\texttt{\{x:\{a:Nat,b:Nat\},y:\{m:Nat\}\}} <: \texttt{\{x:\{a:Nat\}\}}}\ \textsc{S-Trans}$$

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 super*class* ("single inheritance" of classes)

  $\longrightarrow$ *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

$$\frac{\mathtt{T}_1 <: \mathtt{S}_1 \qquad \mathtt{S}_2 <: \mathtt{T}_2}{\mathtt{S}_1 \rightarrow \mathtt{S}_2 <: \mathtt{T}_1 \rightarrow \mathtt{T}_2} \qquad \text{(S-Arrow)}$$

Note the order of $\mathtt{T}_1$ and $\mathtt{S}_1$ 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 $\mathtt{f}$ of type $\mathtt{S}_1 \rightarrow \mathtt{S}_2$, then we know that $\mathtt{f}$ accepts elements of type $\mathtt{S}_1$; clearly, $\mathtt{f}$ will also accept elements of any subtype $\mathtt{T}_1$ of $\mathtt{S}_1$. The type of $\mathtt{f}$ also tells us that it returns elements of type $\mathtt{S}_2$; we can also view these results belonging to any supertype $\mathtt{T}_2$ of $\mathtt{S}_2$. That is, any function $\mathtt{f}$ of type $\mathtt{S}_1 \rightarrow \mathtt{S}_2$ can also be viewed as having type $\mathtt{T}_1 \rightarrow \mathtt{T}_2$.

Intuition of the S-Arrow rule:
“eats less, produces more” is always welcome. :)

```
  C<:A    B<:D                             c<a   b<d
----------------- S-Arrow   analogous to  ------------
  A->B <: C->D                             b/a < d/c
```

f: {x:Nat}->{y:Bool} can be used as input to g:

```
g = \p:{x:Nat,z:Nat}->{}. q (p {x=5,z=2})
```

(g f) typechecks because 1. f can be used in place of p:

   f expects {x:Nat} so {x=5,z=2} is a good input to f.

   (contra-variant on input).

2. on the other hand, (p {x=5,z=2}) returns type {} which is
   the input type of q.

   f {x=5,z=2} outputs type {y:Bool} which is a good input to q.

eating {x:Nat} and producing {y:Bool} is always welcome in a
context which expects you to eat {x:Nat,z:Nat} and produce {}.

Motivation now let's typecheck this example

With our usual typing rule for applications

$$\frac{\Gamma \vdash \mathtt{t}_1 : \mathtt{T}_{11} \to \mathtt{T}_{12} \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T}_{11}}{\Gamma \vdash \mathtt{t}_1\ \mathtt{t}_2 : \mathtt{T}_{12}} \qquad \text{(T-App)}$$

the term

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

is *not* well typed.

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.

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

Cf. `Object` in Java.

The Subtype Relation: General rules

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

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

Subtype relation

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

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

$$\{\mathtt{l}_i\mathtt{:T}_i\ ^{i\in 1..n+k}\} <: \{\mathtt{l}_i\mathtt{:T}_i\ ^{i\in 1..n}\} \qquad \text{(S-RcdWidth)}$$

$$\frac{\text{for each } i \qquad \mathtt{S}_i <: \mathtt{T}_i}{\{\mathtt{l}_i\mathtt{:S}_i\ ^{i\in 1..n}\} <: \{\mathtt{l}_i\mathtt{:T}_i\ ^{i\in 1..n}\}} \qquad \text{(S-RcdDepth)}$$

$$\frac{\{\mathtt{k}_j\mathtt{:S}_j\ ^{j\in 1..n}\} \text{ is a permutation of } \{\mathtt{l}_i\mathtt{:T}_i\ ^{i\in 1..n}\}}{\{\mathtt{k}_j\mathtt{:S}_j\ ^{j\in 1..n}\} <: \{\mathtt{l}_i\mathtt{:T}_i\ ^{i\in 1..n}\}} \qquad \text{(S-RcdPerm)}$$

$$\frac{\mathtt{T}_1 <: \mathtt{S}_1 \qquad \mathtt{S}_2 <: \mathtt{T}_2}{\mathtt{S}_1 \rightarrow \mathtt{S}_2 <: \mathtt{T}_1 \rightarrow \mathtt{T}_2} \qquad \text{(S-Arrow)}$$

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

Syntax

$t ::=$		*terms:*
	x	*variable*
	$\lambda x{:}T.t$	*abstraction*
	$t\ t$	*application*
$v ::=$		*values:*
	$\lambda x{:}T.t$	*abstraction value*
$T ::=$		*types:*
	Top	*maximum type*
	$T \rightarrow T$	*type of functions*
$\Gamma ::=$		*contexts:*
	$\varnothing$	*empty context*
	$\Gamma, x{:}T$	*term variable binding*

Evaluation $\boxed{t \longrightarrow t'}$

$$\frac{t_1 \longrightarrow t_1'}{t_1\ t_2 \longrightarrow t_1'\ t_2} \quad \text{(E-APP1)}$$

$$\frac{t_2 \longrightarrow t_2'}{v_1\ t_2 \longrightarrow v_1\ t_2'} \quad \text{(E-APP2)}$$

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

Subtyping $\boxed{S <: T}$

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

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

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

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

Typing $\boxed{\Gamma \vdash t : T}$

$$\frac{x{:}T \in \Gamma}{\Gamma \vdash x : T} \quad \text{(T-VAR)}$$

$$\frac{\Gamma, x{:}T_1 \vdash t_2 : T_2}{\Gamma \vdash \lambda x{:}T_1.t_2 : T_1 \rightarrow T_2} \quad \text{(T-ABS)}$$

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

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

Figure 15-1: Simply typed lambda-calculus with subtyping ($\lambda_{<:}$)

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.

$$\frac{\Gamma \vdash \mathtt{t} : \mathtt{S} \qquad \mathtt{S} <: \mathtt{T}}{\Gamma \vdash \mathtt{t} : \mathtt{T}} \tag{T-Sub}$$

Preservation

Theorem: If $\Gamma \vdash \mathtt{t} : \mathtt{T}$ and $\mathtt{t} \longrightarrow \mathtt{t}'$, then $\Gamma \vdash \mathtt{t}' : \mathtt{T}$.

Proof: By induction on typing derivations.

(Which cases are likely to be hard?)

Subsumption case

Case T-Sub: $\quad$ `t : S` $\quad$ `S <: T`

Subsumption case

Case T-SUB: $\quad$ `t : S` $\quad$ `S <: T`

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

Subsumption case

Case T-SUB: $\quad$ `t : S` $\quad$ `S <: T`

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

Not hard!

Application case

Case T-App:

$$\mathtt{t} = \mathtt{t}_1\ \mathtt{t}_2 \qquad \Gamma \vdash \mathtt{t}_1 : \mathtt{T}_{11}{\to}\mathtt{T}_{12} \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T}_{11} \qquad \mathtt{T} = \mathtt{T}_{12}$$

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

Application case

Case T-App:

$$\mathtt{t} = \mathtt{t}_1\ \mathtt{t}_2 \qquad \Gamma \vdash \mathtt{t}_1 : \mathtt{T}_{11}{\to}\mathtt{T}_{12} \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T}_{11} \qquad \mathtt{T} = \mathtt{T}_{12}$$

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

Subcase E-App1: $\quad \mathtt{t}_1 \longrightarrow \mathtt{t}_1' \qquad \mathtt{t}' = \mathtt{t}_1'\ \mathtt{t}_2$

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

$$\frac{\Gamma \vdash \mathtt{t}_1 : \mathtt{T}_{11}{\to}\mathtt{T}_{12} \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T}_{11}}{\Gamma \vdash \mathtt{t}_1\ \mathtt{t}_2 : \mathtt{T}_{12}} \qquad \text{(T-App)}$$

Application case

Case T-APP:

$$\mathtt{t} = \mathtt{t}_1\ \mathtt{t}_2 \qquad \Gamma \vdash \mathtt{t}_1 : \mathtt{T}_{11}{\rightarrow}\mathtt{T}_{12} \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T}_{11} \qquad \mathtt{T} = \mathtt{T}_{12}$$

By the inversion lemma for evaluation, there are three rules by which $\mathtt{t} \longrightarrow \mathtt{t}'$ can be derived: E-APP1, E-APP2, and E-APPABS. Proceed by cases.

Subcase E-APP1: $\quad \mathtt{t}_1 \longrightarrow \mathtt{t}_1' \qquad \mathtt{t}' = \mathtt{t}_1'\ \mathtt{t}_2$

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

$$\frac{\Gamma \vdash \mathtt{t}_1 : \mathtt{T}_{11}{\rightarrow}\mathtt{T}_{12} \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T}_{11}}{\Gamma \vdash \mathtt{t}_1\ \mathtt{t}_2 : \mathtt{T}_{12}} \tag{T-App}$$

$$\frac{\mathtt{t}_1 \longrightarrow \mathtt{t}_1'}{\mathtt{t}_1\ \mathtt{t}_2 \longrightarrow \mathtt{t}_1'\ \mathtt{t}_2} \tag{E-App1}$$

Case T-App (continued):

$\mathtt{t} = \mathtt{t}_1\ \mathtt{t}_2 \qquad \Gamma \vdash \mathtt{t}_1 : \mathtt{T}_{11}{\to}\mathtt{T}_{12} \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T}_{11} \qquad \mathtt{T} = \mathtt{T}_{12}$

Subcase E-App2: $\quad \mathtt{t}_1 = \mathtt{v}_1 \qquad \mathtt{t}_2 \longrightarrow \mathtt{t}_2' \qquad \mathtt{t}' = \mathtt{v}_1\ \mathtt{t}_2'$

Similar.

$$\frac{\Gamma \vdash \mathtt{t}_1 : \mathtt{T}_{11}{\to}\mathtt{T}_{12} \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T}_{11}}{\Gamma \vdash \mathtt{t}_1\ \mathtt{t}_2 : \mathtt{T}_{12}} \qquad \text{(T-App)}$$

$$\frac{\mathtt{t}_2 \longrightarrow \mathtt{t}_2'}{\mathtt{v}_1\ \mathtt{t}_2 \longrightarrow \mathtt{v}_1\ \mathtt{t}_2'} \qquad \text{(E-App2)}$$

Case T-App (continued):

$\mathtt{t} = \mathtt{t}_1\ \mathtt{t}_2 \qquad \Gamma \vdash \mathtt{t}_1 : \mathtt{T}_{11}{\to}\mathtt{T}_{12} \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T}_{11} \qquad \mathtt{T} = \mathtt{T}_{12}$

Subcase E-AppAbs:

$\mathtt{t}_1 = \lambda\mathtt{x}{:}\mathtt{S}_{11}.\ \mathtt{t}_{12} \qquad \mathtt{t}_2 = \mathtt{v}_2 \qquad \mathtt{t}' = [\mathtt{x} \mapsto \mathtt{v}_2]\mathtt{t}_{12}$

By the inversion lemma for the typing relation...

Case T-APP (CONTINUED):

$\mathtt{t} = \mathtt{t}_1\ \mathtt{t}_2 \qquad \Gamma \vdash \mathtt{t}_1 : \mathtt{T}_{11} \to \mathtt{T}_{12} \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T}_{11} \qquad \mathtt{T} = \mathtt{T}_{12}$

Subcase E-APPABS:

$\mathtt{t}_1 = \lambda \mathtt{x}{:}\mathtt{S}_{11}.\ \mathtt{t}_{12} \qquad \mathtt{t}_2 = \mathtt{v}_2 \qquad \mathtt{t}' = [\mathtt{x} \mapsto \mathtt{v}_2]\mathtt{t}_{12}$

By the inversion lemma for the typing relation... $\mathtt{T}_{11} <: \mathtt{S}_{11}$ and $\Gamma, \mathtt{x}{:}\mathtt{S}_{11} \vdash \mathtt{t}_{12} : \mathtt{T}_{12}$.

Case T-App (continued):

$$\mathtt{t} = \mathtt{t}_1\ \mathtt{t}_2 \qquad \Gamma \vdash \mathtt{t}_1 : \mathtt{T}_{11}{\to}\mathtt{T}_{12} \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T}_{11} \qquad \mathtt{T} = \mathtt{T}_{12}$$

Subcase E-AppAbs:

$$\mathtt{t}_1 = \lambda\mathtt{x}{:}\mathtt{S}_{11}.\ \mathtt{t}_{12} \qquad \mathtt{t}_2 = \mathtt{v}_2 \qquad \mathtt{t}' = [\mathtt{x} \mapsto \mathtt{v}_2]\mathtt{t}_{12}$$

By the inversion lemma for the typing relation... $\mathtt{T}_{11} <: \mathtt{S}_{11}$ and $\Gamma, \mathtt{x}{:}\mathtt{S}_{11} \vdash \mathtt{t}_{12} : \mathtt{T}_{12}$.

By T-Sub, $\Gamma \vdash \mathtt{t}_2 : \mathtt{S}_{11}$.

Case T-App (continued):

$\mathtt{t} = \mathtt{t}_1\ \mathtt{t}_2 \qquad \Gamma \vdash \mathtt{t}_1 : \mathtt{T}_{11}{\rightarrow}\mathtt{T}_{12} \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T}_{11} \qquad \mathtt{T} = \mathtt{T}_{12}$

Subcase E-AppAbs:

$\mathtt{t}_1 = \lambda\mathtt{x}{:}\mathtt{S}_{11}.\ \mathtt{t}_{12} \qquad \mathtt{t}_2 = \mathtt{v}_2 \qquad \mathtt{t}' = [\mathtt{x} \mapsto \mathtt{v}_2]\mathtt{t}_{12}$

By the inversion lemma for the typing relation... $\mathtt{T}_{11}$ <: $\mathtt{S}_{11}$ and $\Gamma, \mathtt{x}{:}\mathtt{S}_{11} \vdash \mathtt{t}_{12} : \mathtt{T}_{12}$.
By T-Sub, $\Gamma \vdash \mathtt{t}_2 : \mathtt{S}_{11}$.
By the substitution lemma, $\Gamma \vdash \mathtt{t}' : \mathtt{T}_{12}$, and we are done.

$$\frac{\Gamma \vdash \mathtt{t}_1 : \mathtt{T}_{11}{\rightarrow}\mathtt{T}_{12} \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T}_{11}}{\Gamma \vdash \mathtt{t}_1\ \mathtt{t}_2 : \mathtt{T}_{12}} \tag{T-App}$$

$$(\lambda\mathtt{x}{:}\mathtt{T}_{11}.\mathtt{t}_{12})\ \mathtt{v}_2 \longrightarrow [\mathtt{x} \mapsto \mathtt{v}_2]\mathtt{t}_{12} \tag{E-AppAbs}$$

Lemma:

1. If $\Gamma \vdash \texttt{true} : \texttt{R}$, then $\texttt{R} = \texttt{Bool}$.
2. If $\Gamma \vdash \texttt{false} : \texttt{R}$, then $\texttt{R} = \texttt{Bool}$.
3. If $\Gamma \vdash \texttt{if } \texttt{t}_1 \texttt{ then } \texttt{t}_2 \texttt{ else } \texttt{t}_3 : \texttt{R}$, then $\Gamma \vdash \texttt{t}_1 : \texttt{Bool}$ and $\Gamma \vdash \texttt{t}_2, \texttt{t}_3 : \texttt{R}$.
4. If $\Gamma \vdash \texttt{x} : \texttt{R}$, then $\texttt{x}{:}\texttt{R} \in \Gamma$.
5. If $\Gamma \vdash \lambda\texttt{x}{:}\texttt{T}_1.\texttt{t}_2 : \texttt{R}$, then $\texttt{R} = \texttt{T}_1 {\rightarrow} \texttt{R}_2$ for some $\texttt{R}_2$ with $\Gamma, \texttt{x}{:}\texttt{T}_1 \vdash \texttt{t}_2 : \texttt{R}_2$.
6. If $\Gamma \vdash \texttt{t}_1\ \texttt{t}_2 : \texttt{R}$, then there is some type $\texttt{T}_{11}$ such that $\Gamma \vdash \texttt{t}_1 : \texttt{T}_{11} {\rightarrow} \texttt{R}$ and $\Gamma \vdash \texttt{t}_2 : \texttt{T}_{11}$.

Inversion Lemma for

5. If $\Gamma \vdash \lambda x{:}T_1.t_2 : R$, then $R = T_1 \to R_2$ for some R_2 with $\Gamma, x{:}T_1 \vdash t_2 : R_2$.

Lemma: If $\Gamma \vdash \lambda x{:}S_1.s_2 : T_1 \to T_2$, 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 $\Gamma \vdash \lambda\mathtt{x}{:}\mathtt{S}_1\,.\,\mathtt{s}_2 : \mathtt{T}_1{\to}\mathtt{T}_2$, then $\mathtt{T}_1 <: \mathtt{S}_1$ and $\Gamma, \mathtt{x}{:}\mathtt{S}_1 \vdash \mathtt{s}_2 : \mathtt{T}_2$.

Proof: Induction on typing derivations.

Case T-Sub: $\quad \lambda\mathtt{x}{:}\mathtt{S}_1\,.\,\mathtt{s}_2 : \mathtt{U} \qquad \mathtt{U} <: \mathtt{T}_1{\to}\mathtt{T}_2$

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: $\lambda x{:}S_1.s_2 : U \qquad U <: T_1{\rightarrow}T_2$

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 $\Gamma \vdash \lambda \mathtt{x}{:}\mathtt{S}_1\mathtt{.s}_2 : \mathtt{T}_1 \to \mathtt{T}_2$, then $\mathtt{T}_1 <: \mathtt{S}_1$ and $\Gamma, \mathtt{x}{:}\mathtt{S}_1 \vdash \mathtt{s}_2 : \mathtt{T}_2$.
Proof: Induction on typing derivations.

Case T-SUB: $\quad \lambda \mathtt{x}{:}\mathtt{S}_1\mathtt{.s}_2 : \mathtt{U} \qquad \mathtt{U} <: \mathtt{T}_1 \to \mathtt{T}_2$

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

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

Inversion Lemma for Typing

Lemma: If $\Gamma \vdash \lambda\mathtt{x}{:}\mathtt{S}_1\,.\,\mathtt{s}_2 : \mathtt{T}_1{\rightarrow}\mathtt{T}_2$, then $\mathtt{T}_1 <: \mathtt{S}_1$ and $\Gamma, \mathtt{x}{:}\mathtt{S}_1 \vdash \mathtt{s}_2 : \mathtt{T}_2$.

Proof: Induction on typing derivations.

Case T-SUB: $\quad \lambda\mathtt{x}{:}\mathtt{S}_1\,.\,\mathtt{s}_2 : \mathtt{U} \qquad \mathtt{U} <: \mathtt{T}_1{\rightarrow}\mathtt{T}_2$

We want to say "By the induction hypothesis...", but the IH does not apply (we do not know that $\mathtt{U}$ 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 $\mathtt{U} = \mathtt{U}_1{\rightarrow}\mathtt{U}_2$, with $\mathtt{T}_1 <: \mathtt{U}_1$ and $\mathtt{U}_2 <: \mathtt{T}_2$.

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: $\quad \lambda x{:}S_1.s_2 : U \qquad U <: T_1 \rightarrow T_2$

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 $\Gamma \vdash \lambda\mathtt{x}{:}\mathtt{S}_1\,.\,\mathtt{s}_2 : \mathtt{T}_1 \rightarrow \mathtt{T}_2$, then $\mathtt{T}_1 <: \mathtt{S}_1$ and $\Gamma, \mathtt{x}{:}\mathtt{S}_1 \vdash \mathtt{s}_2 : \mathtt{T}_2$.

Proof: Induction on typing derivations.

Case T-SUB: $\qquad \lambda\mathtt{x}{:}\mathtt{S}_1\,.\,\mathtt{s}_2 : \mathtt{U} \qquad \mathtt{U} <: \mathtt{T}_1 \rightarrow \mathtt{T}_2$

We want to say "By the induction hypothesis...", but the IH does not apply (we do not know that $\mathtt{U}$ 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 $\mathtt{U} = \mathtt{U}_1 \rightarrow \mathtt{U}_2$, with $\mathtt{T}_1 <: \mathtt{U}_1$ and $\mathtt{U}_2 <: \mathtt{T}_2$.
The IH now applies, yielding $\mathtt{U}_1 <: \mathtt{S}_1$ and $\Gamma, \mathtt{x}{:}\mathtt{S}_1 \vdash \mathtt{s}_2 : \mathtt{U}_2$.
From $\mathtt{U}_1 <: \mathtt{S}_1$ and $\mathtt{T}_1 <: \mathtt{U}_1$, rule S-TRANS gives $\mathtt{T}_1 <: \mathtt{S}_1$.

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: $\quad \lambda x{:}S_1.s_2 : U \qquad U <: T_1 \rightarrow T_2$

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:

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

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

Ascription and Casting

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma \vdash t : S} \qquad \dfrac{\vdots}{S <: T}}{\Gamma \vdash t : T}\;\text{T-SUB}}{\Gamma \vdash t \text{ as } T : T}\;\text{T-ASCRIBE}$$

Ordinary ascription: **(upcasting)**

$$\frac{\Gamma \vdash t_1 : T}{\Gamma \vdash t_1 \text{ as } T : T} \qquad \text{(T-ASCRIBE)}$$

$$v_1 \text{ as } T \longrightarrow v_1 \qquad \text{(E-ASCRIBE)}$$

Casting (cf. Java): **(downcasting)**

```
f = λ(x:Top) (x as {a:Nat}).a;
```

trust (at compile time)

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

but

verify (at run time)

$$\frac{\vdash v_1 : T}{v_1 \text{ as } T \longrightarrow v_1} \qquad \text{(E-CAST)}$$

does progress theorem still hold?

Subtyping and Variants

$$\texttt{<}\texttt{l}_i\texttt{:}\texttt{T}_i\ {}^{i\in 1..n}\texttt{>} \quad <: \quad \texttt{<}\texttt{l}_i\texttt{:}\texttt{T}_i\ {}^{i\in 1..n+k}\texttt{>} \qquad \text{(S-VariantWidth)}$$

$$\frac{\text{for each } i \quad \texttt{S}_i <: \texttt{T}_i}{\texttt{<}\texttt{l}_i\texttt{:}\texttt{S}_i\ {}^{i\in 1..n}\texttt{>} \quad <: \quad \texttt{<}\texttt{l}_i\texttt{:}\texttt{T}_i\ {}^{i\in 1..n}\texttt{>}} \qquad \text{(S-VariantDepth)}$$

$$\frac{\texttt{<}\texttt{k}_j\texttt{:}\texttt{S}_j\ {}^{j\in 1..n}\texttt{>} \text{ is a permutation of } \texttt{<}\texttt{l}_i\texttt{:}\texttt{T}_i\ {}^{i\in 1..n}\texttt{>}}{\texttt{<}\texttt{k}_j\texttt{:}\texttt{S}_j\ {}^{j\in 1..n}\texttt{>} \quad <: \quad \texttt{<}\texttt{l}_i\texttt{:}\texttt{T}_i\ {}^{i\in 1..n}\texttt{>}} \qquad \text{(S-VariantPerm)}$$

$$\frac{\Gamma \vdash \texttt{t}_1 : \texttt{T}_1}{\Gamma \vdash \texttt{<}\texttt{l}_1\texttt{=}\texttt{t}_1\texttt{>} : \texttt{<}\texttt{l}_1\texttt{:}\texttt{T}_1\texttt{>}} \qquad \text{(T-Variant)}$$

Subtyping and Lists

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

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

Subtyping and References

$$\frac{\texttt{S}_1 \mathrel{\texttt{<:}} \texttt{T}_1 \qquad \texttt{T}_1 \mathrel{\texttt{<:}} \texttt{S}_1}{\texttt{Ref S}_1 \mathrel{\texttt{<:}} \texttt{Ref T}_1} \quad \text{(S-R}\textsc{ef}\text{)}$$

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

Subtyping and References

$$\frac{\texttt{S}_1 \mathrel{\texttt{<:}} \texttt{T}_1 \qquad \texttt{T}_1 \mathrel{\texttt{<:}} \texttt{S}_1}{\texttt{Ref}\ \texttt{S}_1 \mathrel{\texttt{<:}} \texttt{Ref}\ \texttt{T}_1} \tag{S-Ref}$$

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

- When a reference is *read*, the context expects a $\texttt{T}_1$, so if $\texttt{S}_1 \mathrel{\texttt{<:}} \texttt{T}_1$ then an $\texttt{S}_1$ is ok.

Subtyping and References

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

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

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

Subtyping and Arrays

array is mutable, list is immutable

Similarly...

$$\frac{\mathtt{S_1} <: \mathtt{T_1} \qquad \mathtt{T_1} <: \mathtt{S_1}}{\mathtt{Array}\ \mathtt{S_1} <: \mathtt{Array}\ \mathtt{T_1}} \qquad \text{(S-ARRAY)}$$

Subtyping and Arrays

array is mutable, list is immutable

Similarly...

$$\frac{\texttt{S}_1 \texttt{ <: } \texttt{T}_1 \qquad \texttt{T}_1 \texttt{ <: } \texttt{S}_1}{\texttt{Array } \texttt{S}_1 \texttt{ <: } \texttt{Array } \texttt{T}_1} \quad \text{(S-Array)}$$

$$\frac{\texttt{S}_1 \texttt{ <: } \texttt{T}_1}{\texttt{Array } \texttt{S}_1 \texttt{ <: } \texttt{Array } \texttt{T}_1} \quad \text{(S-ArrayJava)}$$

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

in Java syntax, S1[] <: T1[]

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

$$\frac{\Gamma \mid \Sigma \vdash \mathtt{t}_1 : \mathtt{Source}\ \mathtt{T}_{11}}{\Gamma \mid \Sigma \vdash \mathtt{!t}_1 : \mathtt{T}_{11}} \quad \text{(T-Deref)}$$

$$\frac{\Gamma \mid \Sigma \vdash \mathtt{t}_1 : \mathtt{Sink}\ \mathtt{T}_{11} \qquad \Gamma \mid \Sigma \vdash \mathtt{t}_2 : \mathtt{T}_{11}}{\Gamma \mid \Sigma \vdash \mathtt{t}_1\mathtt{:=}\mathtt{t}_2 : \mathtt{Unit}} \quad \text{(T-Assign)}$$

Subtyping rules

$$\frac{\texttt{S}_1 \texttt{ <: } \texttt{T}_1}{\texttt{Source S}_1 \texttt{ <: } \texttt{Source T}_1} \qquad (\textsc{S-Source})$$

$$\frac{\texttt{T}_1 \texttt{ <: } \texttt{S}_1}{\texttt{Sink S}_1 \texttt{ <: } \texttt{Sink T}_1} \qquad (\textsc{S-Sink})$$

$$\texttt{Ref T}_1 \texttt{ <: } \texttt{Source T}_1 \qquad (\textsc{S-RefSource})$$

$$\texttt{Ref T}_1 \texttt{ <: } \texttt{Sink T}_1 \qquad (\textsc{S-RefSink})$$

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.

$$\frac{\Gamma \vdash \mathtt{t}_1 : \mathtt{T}_{11} \to \mathtt{T}_{12} \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T}_{11}}{\Gamma \vdash \mathtt{t}_1\ \mathtt{t}_2 : \mathtt{T}_{12}} \qquad \text{(T-App)}$$

If we are given some Γ and some $\mathtt{t}$ of the form $\mathtt{t}_1\ \mathtt{t}_2$, we can try to find a type for $\mathtt{t}$ by

1. finding (recursively) a type for $\mathtt{t}_1$
2. checking that it has the form $\mathtt{T}_{11} \to \mathtt{T}_{12}$
3. finding (recursively) a type for $\mathtt{t}_2$
4. checking that it is the same as $\mathtt{T}_{11}$

Technically, the reason this works is that We can divide the "positions" of the typing relation into *input positions* (Γ and $\mathtt{t}$) and *output positions* ($\mathtt{T}$).

- 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)

$$\frac{\Gamma \vdash \mathtt{t}_1 : \mathtt{T}_{11} \to \mathtt{T}_{12} \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T}_{11}}{\Gamma \vdash \mathtt{t}_1\ \mathtt{t}_2 : \mathtt{T}_{12}} \qquad (\text{T-App})$$

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" Γ 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.

$\longrightarrow$ 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)

$$\frac{\Gamma \vdash \mathtt{t} : \mathtt{S} \qquad \mathtt{S} <: \mathtt{T}}{\Gamma \vdash \mathtt{t} : \mathtt{T}} \qquad \text{(T-SUB)}$$

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

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

   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?

What to do?

1. Observation: We don't *need* 1000 ways to prove a given typing or subtyping statement — one is enough.
   $\longrightarrow$ 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.

Developing an algorithmic subtyping relation

Subtype relation

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

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

$$\{\texttt{l}_i\texttt{:T}_i\ ^{i\in 1..n+k}\} <: \{\texttt{l}_i\texttt{:T}_i\ ^{i\in 1..n}\} \qquad \text{(S-RcdWidth)}$$

$$\frac{\text{for each } i \qquad \texttt{S}_i <: \texttt{T}_i}{\{\texttt{l}_i\texttt{:S}_i\ ^{i\in 1..n}\} <: \{\texttt{l}_i\texttt{:T}_i\ ^{i\in 1..n}\}} \qquad \text{(S-RcdDepth)}$$

$$\frac{\{\texttt{k}_j\texttt{:S}_j\ ^{j\in 1..n}\} \text{ is a permutation of } \{\texttt{l}_i\texttt{:T}_i\ ^{i\in 1..n}\}}{\{\texttt{k}_j\texttt{:S}_j\ ^{j\in 1..n}\} <: \{\texttt{l}_i\texttt{:T}_i\ ^{i\in 1..n}\}} \qquad \text{(S-RcdPerm)}$$

$$\frac{\texttt{T}_1 <: \texttt{S}_1 \qquad \texttt{S}_2 <: \texttt{T}_2}{\texttt{S}_1 \to \texttt{S}_2 <: \texttt{T}_1 \to \texttt{T}_2} \qquad \text{(S-Arrow)}$$

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

Issues

For a given subtyping statement, there are multiple rules that could be used last in a derivation.

1. The conclusions of S-RcdWidth, S-RcdDepth, and S-RcdPerm overlap with each other.
2. S-Refl and S-Trans overlap with every other rule.

Step 1: simplify record subtyping

Idea: combine all three record subtyping rules into one "macro rule" that captures all of their effects

$$\frac{\{\mathtt{l}_i{}^{\,i\in 1..n}\} \subseteq \{\mathtt{k}_j{}^{\,j\in 1..m}\} \qquad \mathtt{k}_j = \mathtt{l}_i \text{ implies } \mathtt{S}_j <: \mathtt{T}_i}{\{\mathtt{k}_j\!:\!\mathtt{S}_j{}^{\,j\in 1..m}\} <: \{\mathtt{l}_i\!:\!\mathtt{T}_i{}^{\,i\in 1..n}\}} \qquad \text{(S-RCD)}$$

Simpler subtype relation

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

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

$$\frac{\{\mathtt{l}_i\ ^{i\in 1..n}\} \subseteq \{\mathtt{k}_j\ ^{j\in 1..m}\} \qquad \mathtt{k}_j = \mathtt{l}_i \text{ implies } \mathtt{S}_j <: \mathtt{T}_i}{\{\mathtt{k}_j\!:\!\mathtt{S}_j\ ^{j\in 1..m}\} <: \{\mathtt{l}_i\!:\!\mathtt{T}_i\ ^{i\in 1..n}\}} \qquad \text{(S-Rcd)}$$

$$\frac{\mathtt{T}_1 <: \mathtt{S}_1 \qquad \mathtt{S}_2 <: \mathtt{T}_2}{\mathtt{S}_1 \to \mathtt{S}_2 <: \mathtt{T}_1 \to \mathtt{T}_2} \qquad \text{(S-Arrow)}$$

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

Step 2: Get rid of reflexivity

Observation: S-Refl is unnecessary.

Lemma: $S <: S$ can be derived for every type S without using S-Refl.

Even simpler subtype relation

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

$$\frac{\{\mathtt{l}_i{}^{i\in 1..n}\} \subseteq \{\mathtt{k}_j{}^{j\in 1..m}\} \qquad \mathtt{k}_j = \mathtt{l}_i \text{ implies } \mathtt{S}_j <: \mathtt{T}_i}{\{\mathtt{k}_j\mathtt{:}\mathtt{S}_j{}^{j\in 1..m}\} <: \{\mathtt{l}_i\mathtt{:}\mathtt{T}_i{}^{i\in 1..n}\}} \qquad \text{(S-Rcd)}$$

$$\frac{\mathtt{T}_1 <: \mathtt{S}_1 \qquad \mathtt{S}_2 <: \mathtt{T}_2}{\mathtt{S}_1 \to \mathtt{S}_2 <: \mathtt{T}_1 \to \mathtt{T}_2} \qquad \text{(S-Arrow)}$$

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

Step 3: Get rid of transitivity

Observation: S-Trans is unnecessary.

Lemma: If `S <: T` can be derived, then it can be derived without using S-Trans.

"Algorithmic" subtype relation

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

$$\frac{\mapsto \texttt{T}_1 <: \texttt{S}_1 \qquad \mapsto \texttt{S}_2 <: \texttt{T}_2}{\mapsto \texttt{S}_1 \rightarrow \texttt{S}_2 <: \texttt{T}_1 \rightarrow \texttt{T}_2} \qquad \text{(SA-Arrow)}$$

$$\frac{\{\texttt{l}_i \ ^{i \in 1..n}\} \subseteq \{\texttt{k}_j \ ^{j \in 1..m}\} \qquad \text{for each } \texttt{k}_j = \texttt{l}_i,\ \mapsto \texttt{S}_j <: \texttt{T}_i}{\mapsto \{\texttt{k}_j \texttt{:} \texttt{S}_j \ ^{j \in 1..m}\} <: \{\texttt{l}_i \texttt{:} \texttt{T}_i \ ^{i \in 1..n}\}} \qquad \text{(SA-Rcd)}$$

Soundness and completeness

Theorem: $\mathtt{S} <: \mathtt{T}$ iff $\blacktriangleright \mathtt{S} <: \mathtt{T}$.

Proof: *(Homework)*

Terminology:

- The algorithmic presentation of subtyping is *sound* with respect to the original if $\blacktriangleright \mathtt{S} <: \mathtt{T}$ implies $\mathtt{S} <: \mathtt{T}$. (Everything validated by the algorithm is actually true.)
- The algorithmic presentation of subtyping is *complete* with respect to the original if $\mathtt{S} <: \mathtt{T}$ implies $\blacktriangleright \mathtt{S} <: \mathtt{T}$. (Everything true is validated by the algorithm.)

Subtyping Algorithm (pseudo-code)

The algorithmic rules can be translated directly into code:

$\mathit{subtype}(\mathtt{S}, \mathtt{T}) \;\; =$

if $\mathtt{T} = \mathtt{Top}$, then *true*

else if $\mathtt{S} = \mathtt{S}_1 \rightarrow \mathtt{S}_2$ and $\mathtt{T} = \mathtt{T}_1 \rightarrow \mathtt{T}_2$

then $\mathit{subtype}(\mathtt{T}_1, \mathtt{S}_1) \;\wedge\; \mathit{subtype}(\mathtt{S}_2, \mathtt{T}_2)$

else if $\mathtt{S} = \{\mathtt{k}_j \mathtt{:} \mathtt{S}_j \;^{j \in 1..m}\}$ and $\mathtt{T} = \{\mathtt{l}_i \mathtt{:} \mathtt{T}_i \;^{i \in 1..n}\}$

then $\{\mathtt{l}_i \;^{i \in 1..n}\} \subseteq \{\mathtt{k}_j \;^{j \in 1..m}\}$

$\wedge$ for all $i \in 1..n$ there is some $j \in 1..m$ with $\mathtt{k}_j = \mathtt{l}_i$

and $\mathit{subtype}(\mathtt{S}_j, \mathtt{T}_i)$

else *false*.

Decision Procedures

Recall: A *decision procedure* for a relation $R \subseteq U$ is a total function p from U to $\{\mathit{true}, \mathit{false}\}$ such that $p(u) = \mathit{true}$ iff $u \in R$.

Decision Procedures

Recall: A *decision procedure* for a relation $R \subseteq U$ is a total function p from U to $\{\mathit{true}, \mathit{false}\}$ such that $p(u) = \mathit{true}$ iff $u \in R$.

Is our *subtype* function a decision procedure?

Decision Procedures

Recall: A *decision procedure* for a relation $R \subseteq U$ is a total function p from U to $\{\mathit{true}, \mathit{false}\}$ such that $p(u) = \mathit{true}$ iff $u \in R$.

Is our *subtype* function a decision procedure?

Since *subtype* is just an implementation of the algorithmic subtyping rules, we have

1. if $\mathit{subtype}(\mathtt{S}, \mathtt{T}) = \mathit{true}$, then $\mapsto \mathtt{S} <: \mathtt{T}$
   (hence, by soundness of the algorithmic rules, $\mathtt{S} <: \mathtt{T}$)
2. if $\mathit{subtype}(\mathtt{S}, \mathtt{T}) = \mathit{false}$, then not $\mapsto \mathtt{S} <: \mathtt{T}$
   (hence, by completeness of the algorithmic rules, not $\mathtt{S} <: \mathtt{T}$)

Decision Procedures

Recall: A *decision procedure* for a relation $R \subseteq U$ is a total function p from U to $\{true, false\}$ such that $p(u) = true$ iff $u \in R$.

Is our *subtype* function a decision procedure?

Since *subtype* is just an implementation of the algorithmic subtyping rules, we have

1. if $subtype(\texttt{S}, \texttt{T}) = true$, then $\mapsto \texttt{S} <: \texttt{T}$
   (hence, by soundness of the algorithmic rules, $\texttt{S} <: \texttt{T}$)
2. if $subtype(\texttt{S}, \texttt{T}) = false$, then not $\mapsto \texttt{S} <: \texttt{T}$
   (hence, by completeness of the algorithmic rules, not $\texttt{S} <: \texttt{T}$)

Q: What's missing?

Decision Procedures

Recall: A *decision procedure* for a relation $R \subseteq U$ is a total function p from U to $\{true, false\}$ such that $p(u) = true$ iff $u \in R$.

Is our *subtype* function a decision procedure?

Since *subtype* is just an implementation of the algorithmic subtyping rules, we have

1. if $subtype(\mathtt{S}, \mathtt{T}) = true$, then $\mapsto \mathtt{S} <: \mathtt{T}$
   (hence, by soundness of the algorithmic rules, $\mathtt{S} <: \mathtt{T}$)
2. if $subtype(\mathtt{S}, \mathtt{T}) = false$, then not $\mapsto \mathtt{S} <: \mathtt{T}$
   (hence, by completeness of the algorithmic rules, not $\mathtt{S} <: \mathtt{T}$)

Q: What's missing?

A: How do we know that *subtype* is a *total* function?

Decision Procedures

Recall: A *decision procedure* for a relation $R \subseteq U$ is a total function p from U to $\{true, false\}$ such that $p(u) = true$ iff $u \in R$.

Is our *subtype* function a decision procedure?

Since *subtype* is just an implementation of the algorithmic subtyping rules, we have

1. if $subtype(\mathtt{S}, \mathtt{T}) = true$, then $\mapsto \mathtt{S} <: \mathtt{T}$
   (hence, by soundness of the algorithmic rules, $\mathtt{S} <: \mathtt{T}$)
2. if $subtype(\mathtt{S}, \mathtt{T}) = false$, then not $\mapsto \mathtt{S} <: \mathtt{T}$
   (hence, by completeness of the algorithmic rules, not $\mathtt{S} <: \mathtt{T}$)

Q: What's missing?

A: How do we know that *subtype* is a *total* function?

Prove it!

Metatheory of Typing

Issue

For the typing relation, we have just one problematic rule to deal with: subsumption.

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

Where is this rule really needed?

Issue

For the typing relation, we have just one problematic rule to deal with: subsumption.

$$\frac{\Gamma \vdash \mathtt{t} : \mathtt{S} \qquad \mathtt{S} <: \mathtt{T}}{\Gamma \vdash \mathtt{t} : \mathtt{T}} \qquad \text{(T-SUB)}$$

Where is this rule really needed?

For applications. E.g., the term

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

is not typable without using subsumption.

Issue

For the typing relation, we have just one problematic rule to deal with: subsumption.

$$\frac{\Gamma \vdash \mathtt{t} : \mathtt{S} \qquad \mathtt{S} <: \mathtt{T}}{\Gamma \vdash \mathtt{t} : \mathtt{T}} \tag{T-Sub}$$

Where is this rule really needed?

For applications. E.g., the term

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

is not typable without using subsumption.

Where else??

Issue

For the typing relation, we have just one problematic rule to deal with: subsumption.

$$\frac{\Gamma \vdash \mathtt{t} : \mathtt{S} \qquad \mathtt{S} <: \mathtt{T}}{\Gamma \vdash \mathtt{t} : \mathtt{T}} \tag{T-Sub}$$

Where is this rule really needed?

For applications. E.g., the term

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

is not typable without using subsumption.

Where else??

Nowhere else! Uses of subsumption to help typecheck applications are the only interesting ones.

Example (T-Abs)

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma, \mathtt{x}:\mathtt{S_1} \vdash \mathtt{s_2} : \mathtt{S_2}} \qquad \dfrac{\vdots}{\mathtt{S_2} <: \mathtt{T_2}}}{\Gamma, \mathtt{x}:\mathtt{S_1} \vdash \mathtt{s_2} : \mathtt{T_2}}\ (\text{T-Sub})}{\Gamma \vdash \lambda \mathtt{x}:\mathtt{S_1}.\mathtt{s_2} : \mathtt{S_1} \to \mathtt{T_2}}\ (\text{T-Abs})$$

Example (T-Abs)

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma,\, \mathtt{x}{:}\mathtt{S}_1 \vdash \mathtt{s}_2 : \mathtt{S}_2} \qquad \dfrac{\vdots}{\mathtt{S}_2 <: \mathtt{T}_2}}{\Gamma,\, \mathtt{x}{:}\mathtt{S}_1 \vdash \mathtt{s}_2 : \mathtt{T}_2}\;(\text{T-Sub})}{\Gamma \vdash \lambda \mathtt{x}{:}\mathtt{S}_1 . \mathtt{s}_2 : \mathtt{S}_1 \to \mathtt{T}_2}\;(\text{T-Abs})$$

becomes

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma,\, \mathtt{x}{:}\mathtt{S}_1 \vdash \mathtt{s}_2 : \mathtt{S}_2}}{\Gamma \vdash \lambda \mathtt{x}{:}\mathtt{S}_1 . \mathtt{s}_2 : \mathtt{S}_1 \to \mathtt{S}_2}\;(\text{T-Abs}) \qquad \dfrac{\dfrac{}{\mathtt{S}_1 <: \mathtt{S}_1}\;(\text{S-Refl}) \qquad \dfrac{\vdots}{\mathtt{S}_2 <: \mathtt{T}_2}}{\mathtt{S}_1 \to \mathtt{S}_2 <: \mathtt{S}_1 \to \mathtt{T}_2}\;(\text{S-Arrow})}{\Gamma \vdash \lambda \mathtt{x}{:}\mathtt{S}_1 . \mathtt{s}_2 : \mathtt{S}_1 \to \mathtt{T}_2}\;(\text{T-Sub})$$

Example (T-App on the left)

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma \vdash s_1 : S_{11} \to S_{12}} \qquad \dfrac{\dfrac{\vdots}{T_{11} <: S_{11}} \qquad \dfrac{\vdots}{S_{12} <: T_{12}}}{S_{11} \to S_{12} <: T_{11} \to T_{12}}\ (\text{S-Arrow})}{\Gamma \vdash s_1 : T_{11} \to T_{12}}\ (\text{T-Sub}) \qquad \dfrac{\vdots}{\Gamma \vdash s_2 : T_{11}}}{\Gamma \vdash s_1\ s_2 : T_{12}}\ (\text{T-App})$$

Example (T-App on the left)

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma \vdash s_1 : S_{11} \rightarrow S_{12}} \qquad \dfrac{\dfrac{\vdots}{T_{11} <: S_{11}} \qquad \dfrac{\vdots}{S_{12} <: T_{12}}}{S_{11} \rightarrow S_{12} <: T_{11} \rightarrow T_{12}}\ \text{(S-Arrow)}}{\Gamma \vdash s_1 : T_{11} \rightarrow T_{12}}\ \text{(T-Sub)} \qquad \dfrac{\vdots}{\Gamma \vdash s_2 : T_{11}}}{\Gamma \vdash s_1\ s_2 : T_{12}}\ \text{(T-App)}$$

becomes

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma \vdash s_1 : S_{11} \rightarrow S_{12}} \qquad \dfrac{\dfrac{\vdots}{\Gamma \vdash s_2 : T_{11}} \qquad \dfrac{\vdots}{T_{11} <: S_{11}}}{\Gamma \vdash s_2 : S_{11}}\ \text{(T-Sub)}}{\Gamma \vdash s_1\ s_2 : S_{12}}\ \text{(T-App)} \qquad \dfrac{\vdots}{S_{12} <: T_{12}}}{\Gamma \vdash s_1\ s_2 : T_{12}}\ \text{(T-Sub)}$$

Example (T-App on the right)

$$\dfrac{\dfrac{\vdots}{\Gamma \vdash \mathtt{s}_1 : \mathtt{T}_{11} \rightarrow \mathtt{T}_{12}} \qquad \dfrac{\dfrac{\vdots}{\Gamma \vdash \mathtt{s}_2 : \mathtt{T}_2} \quad \dfrac{\vdots}{\mathtt{T}_2 <: \mathtt{T}_{11}}}{\Gamma \vdash \mathtt{s}_2 : \mathtt{T}_{11}}\ (\text{T-Sub})}{\Gamma \vdash \mathtt{s}_1\ \mathtt{s}_2 : \mathtt{T}_{12}}\ (\text{T-App})$$

Example (T-App on the right)

$$\dfrac{\dfrac{\vdots}{\Gamma \vdash \mathtt{s}_1 : \mathtt{T}_{11}\to\mathtt{T}_{12}} \qquad \dfrac{\dfrac{\vdots}{\Gamma \vdash \mathtt{s}_2 : \mathtt{T}_2} \qquad \dfrac{\vdots}{\mathtt{T}_2 <: \mathtt{T}_{11}}}{\Gamma \vdash \mathtt{s}_2 : \mathtt{T}_{11}}\;(\text{T-Sub})}{\Gamma \vdash \mathtt{s}_1\ \mathtt{s}_2 : \mathtt{T}_{12}}\;(\text{T-App})$$

becomes

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma \vdash \mathtt{s}_1 : \mathtt{T}_{11}\to\mathtt{T}_{12}} \qquad \dfrac{\dfrac{\vdots}{\mathtt{T}_2 <: \mathtt{T}_{11}} \qquad \dfrac{}{\mathtt{T}_{12} <: \mathtt{T}_{12}}\;(\text{S-Refl})}{\mathtt{T}_{11}\to\mathtt{T}_{12} <: \mathtt{T}_2\to\mathtt{T}_{12}}\;(\text{S-Arrow})}{\Gamma \vdash \mathtt{s}_1 : \mathtt{T}_2\to\mathtt{T}_{12}}\;(\text{T-Sub}) \qquad \dfrac{\vdots}{\Gamma \vdash \mathtt{s}_2 : \mathtt{T}_2}}{\Gamma \vdash \mathtt{s}_1\ \mathtt{s}_2 : \mathtt{T}_{12}}\;(\text{T-App})$$

Example (T-Sub)

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma \vdash \mathtt{s} : \mathtt{S}} \qquad \dfrac{\vdots}{\mathtt{S} <: \mathtt{U}}}{\Gamma \vdash \mathtt{s} : \mathtt{U}}\;(\textsc{T-Sub}) \qquad \dfrac{\vdots}{\mathtt{U} <: \mathtt{T}}}{\Gamma \vdash \mathtt{s} : \mathtt{T}}\;(\textsc{T-Sub})$$

Example (T-Sub)

$$
\dfrac{\dfrac{\dfrac{\vdots}{\Gamma \vdash \mathtt{s} : \mathtt{S}} \qquad \dfrac{\vdots}{\mathtt{S} <: \mathtt{U}}}{\Gamma \vdash \mathtt{s} : \mathtt{U}}\,(\textsc{T-Sub}) \qquad \dfrac{\vdots}{\mathtt{U} <: \mathtt{T}}}{\Gamma \vdash \mathtt{s} : \mathtt{T}}\,(\textsc{T-Sub})
$$

becomes

$$
\dfrac{\dfrac{\vdots}{\Gamma \vdash \mathtt{s} : \mathtt{S}} \qquad \dfrac{\dfrac{\vdots}{\mathtt{S} <: \mathtt{U}} \qquad \dfrac{\vdots}{\mathtt{U} <: \mathtt{T}}}{\mathtt{S} <: \mathtt{T}}\,(\textsc{S-Trans})}{\Gamma \vdash \mathtt{s} : \mathtt{T}}\,(\textsc{T-Sub})
$$