Recap on Subtype

Rule of Subsumption

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

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

a value of one type can always safely be used where *a value of the other* **is expected**.

Subtype Relation

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

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

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

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

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

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

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

Properties of Subtyping

Safety

Statements of progress and preservation theorems are ***unchanged*** from $\lambda_{\rightarrow}$

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

i.e., given a derivation, *we don't always know what rule was used* in *the last step*

e.g., the rule T-SUB could appear anywhere

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

An *Inversion Lemma* for subtyping

Lemma: If $U <: T_1 \longrightarrow T_2$, then U has the form $U_1 \longrightarrow U_2$, with $T_1 <: U_1$ and $U_2 <: T_2$.

Proof: *By induction on subtyping derivations*

Case S-Arrow: $U = U_1 \longrightarrow U_2 \qquad T_1 <: U_1 \qquad U_2 <: T_2$

Immediate.

Case S-Refl: $U = T_1 \longrightarrow T_2$

By S-Refl (twice), $T_1 <: T_1$ and $T_2 <: T_2$, as required

Case S-Trans: $U <: W \qquad W <: T_1 \longrightarrow T_2$

- Applying the IH to the second subderivation, we find that W has the form $W_1 \longrightarrow W_2$, with $T_1 <: W_1$ and $W_2 <: T_2$.
- Now the IH applies again (to the first subderivation), telling us that U has the form $U_1 \longrightarrow U_2$, with $W_1 <: U_1$ and $U_2 <: W_2$.
- By S-Trans, $T_1 <: U_1$, and, by S-Trans again, $U_2 <: T_2$, as required.

Inversion Lemma for Typing

Lemma: if $\Gamma \vdash \lambda x{:}S_1.s_2 : T_1 \longrightarrow T_2$, then $T_1 <: S_1$ and $\Gamma, x{:}S_1 \vdash s_2 : T_2$

Proof: *Induction on typing derivations*.

Case T-ABS: $T_1 = S_1$ $T_2 = S_2$ $\Gamma, x{:}S_1 \vdash s_2 : S_2$

Case T–SUB: $\Gamma \vdash \lambda x{:}S_1.s_2 : U$ $U: T_1 \longrightarrow T_2$

- By the subtyping inversion lemma, $U_1 \longrightarrow U_2$, 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 $\Gamma, x{:}S_1 \vdash s_2 : T_2$, thus we are done

Preservation

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

Proof: *induction on typing derivations*.

Which cases are likely to be *hard* ?

Preservation - Subsumption case

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

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

By T-Sub , $\Gamma \vdash t' : T$.

Not hard!

Preservation - Application case

Case T-App :

$$\mathsf{t} \;=\; \mathsf{t}_1 \;\; \mathsf{t}_2$$

$$\Gamma \vdash \mathsf{t}_1 : \mathsf{T}_{11} \longrightarrow \mathsf{T}_{12}$$

$$\Gamma \vdash \mathsf{t}_2 : \mathsf{T}_{11}$$

$$\mathsf{T} \;=\; \mathsf{T}_{12}$$

By the inversion lemma for evaluation, there are

three rules

by which $\mathsf{t} \longrightarrow \mathsf{t}'$ can be derived:

E-APP1, E-APP2, and E-APPABS .

Proceed by cases

Preservation - Application case

Case T-App :

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

By the inversion lemma for evaluation, there are *three rules* by which $t \longrightarrow t'$ can be derived:

E-APP1, E-APP2, and E-APPABS

Proceed by cases.

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

Preservation - Application case

Case T-App :

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

Subcase E-App1 : $t_1 \longrightarrow t'_1$ $t' = t'_1 \ t_2$

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

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

Preservation - Application case

Case T-App :

$$t = t_1 \; t_2$$
$$\Gamma \vdash t_1 : T_{11} \longrightarrow T_{12}$$
$$\Gamma \vdash t_2 : T_{11}$$
$$T = T_{12}$$

<u>*Subcase*</u> E-App2 : $t_1 = v_1 \quad t_2 \longrightarrow t'_2 \quad t' = v_1 \, t'_2$

Similar.

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

$$\frac{t_2 \longrightarrow t_2'}{v_1 \; t_2 \longrightarrow v_1 \; t_2'} \quad \text{(E-App2)}$$

Preservation - Application case

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 using T-Sub, $\Gamma \vdash t_2 : S_{11}$

by the *substitution lemma*, $\Gamma \vdash t' : T_{12}$

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

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

Progress

Lemma for Canonical Forms

1. If v is a closed value of type $T_1 \longrightarrow T_2$, then v has the form $\lambda x{:}S_1.t_2$.
2. If v is a closed value of type $\{l_i{:}T_i^{\,i\in 1..n}\}$, then v has the form $\left\{k_j = v_j^{\,j\in 1..m}\right\}$ with $\{l_i^{\,i\in 1..n}\} \subseteq \{k_a^{\,a\in 1..m}\}$

Possible shapes of values belonging to *arrow* and *record* types.

Based on this *Canonical Forms Lemma*, we can still has the progress theorem and its proof quite close to what we saw in the simply typed lambda-calculus

Subtyping
with
Other Features

Ascription and Casting

Ordinary ascription:

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

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

(T) T

up-cast

down-cast

Ascription and Casting

Ordinary ascription:

$$\frac{\Gamma \vdash \mathtt{t}_1 : \mathtt{T}}{\Gamma \vdash \mathtt{t}_1 \ \mathtt{as}\ \mathtt{T} : \mathtt{T}} \qquad \text{(T-Ascribe)}$$

$$\mathtt{v}_1 \ \mathtt{as}\ \mathtt{T} \longrightarrow \mathtt{v}_1 \qquad \text{(E-Ascribe)}$$

Casting (cf. Java):

$$\frac{\Gamma \vdash \mathtt{t}_1 : \mathtt{S}}{\Gamma \vdash \mathtt{t}_1 \ \mathtt{as}\ \mathtt{T} : \mathtt{T}} \qquad \text{(T-Cast)}$$

$$\boxed{\frac{\vdash \mathtt{v}_1 : \mathtt{T}}{\mathtt{v}_1 \ \mathtt{as}\ \mathtt{T} \longrightarrow \mathtt{v}_1} \qquad \text{(E-Cast)}}$$

Subtyping and Variants

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

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

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

$$\text{(S-VariantPerm)}$$

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

Subtyping and Lists

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

i.e., List is a *covariant type* constructor

Subtyping and References

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

i.e., Ref is *not a covariant* (nor *a contravariant*) type constructor, but an *invariant*

Subtyping and References

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 $\mathrm{S}_1 <: \mathrm{T}_1$ 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 $\mathrm{Ref}\ \mathrm{S}_1$, someone else may use the T_1 as an S_1. So we need $\mathrm{T}_1 <: \mathrm{S}_1$.

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 capability"
- Sink T: reference cell with "write capability"
- 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

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

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

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

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

Subtyping and Arrays

Similarly...

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

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

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

Capabilities

Other kinds of capabilities can be treated similarly, e.g.,

- *send* and *receive* capabilities on communication channels,
- *encrypt*/*decrypt* capabilities of cryptographic keys,
- …

Base Types

For language with a rich set of base types, it's better to introduce primitive subtype relations among them

- e.g., Bool <: Nat

Intersection and Union Types

Intersection Types

The inhabitants of $T_1 \wedge T_2$ are terms belonging to *both* S and T — i.e.,

$T_1 \wedge T_2$ is an order-theoretic meet (*greatest lower bound*) of T_1 and T_2

$$T_1 \wedge T_2 <: T_1 \qquad \text{(S-INTER1)}$$

$$T_1 \wedge T_2 <: T_2 \qquad \text{(S-INTER2)}$$

$$\frac{S <: T_1 \qquad S <: T_2}{S <: T_1 \wedge T_2} \qquad \text{(S-INTER3)}$$

$$\boxed{S \to T_1 \wedge S \to T_2 <: S \to (T_1 \wedge T_2) \qquad \text{(S-INTER4)}}$$

Intersection Types

Intersection types permit a very *flexible form* of *finitary overloading*, e,g, S-Inter4:

$$+ : (\mathtt{Nat} \to \mathtt{Nat} \to \mathtt{Nat}) \land (\mathtt{Float} \to \mathtt{Float} \to \mathtt{Float})$$

This form of overloading is extremely powerful.

Every strongly *normalizing untyped lambda-term* can be typed in *the simply typed lambda-calculus* with intersection types

type reconstruction problem is undecidable

Intersection types *have not been used much* in language designs (too powerful!), but are being *intensively investigated* as type systems *for intermediate languages* in highly optimizing compilers (cf. Church project)

Union types

Union types are also useful.

$T_1 \vee T_2$ is an untagged (non-disjoint) ordinary union of the set of values belonging to T_1 and that of values belonging to T_2.

No tags: no *case* construct. The only operations we can safely perform on elements of $T_1 \vee T_2$ are ones *that make sense for both* T_1 and T_2.

Note well: untagged union types in C are a source of *type safety violations* precisely because they ignores this restriction, allowing any operation on an element of $T_1 \vee T_2$ that makes sense for *either* T_1 or T_2.

Union types are being used recently in type systems for XML processing languages (cf. Xduce, Xtatic).

Varieties of Polymorphism

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

Issues
in
Subtyping

Typing with Subsumption

Principle of safe substitution

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

a value of one can *always safely be used* where *a value of the other* is expected

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, i.e.,

Subtype Relation: General rules

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

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

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

A subtyping is *a binary relation* between *types* that is closed under the following rules

Issues in Subtyping

For a *given subtyping statement*, there are *multiple rules* that could be used 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.

Syntax-directed rules

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

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

If we are given some Γ 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 $T_{11} \longrightarrow T_{12}$
3. finding (recursively) a type for t_2
4. checking that it is the same as T_{11}

Syntax-directed rules

Technically, the reason this works is that we can *divide the "**positions**" of the typing relation into **input positions** (i.e., Γ 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)

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

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*:

- for every "*input*" Γ and t, *there is 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* + *T-SUB*)

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

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 translate 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 (∵ 8.2.4 /9.3.3 [uniqueness of types] ×)
2. The transitivity rule

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

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 have to *guess* a value for U!

What to do?

We'll turn the *declarative version* of subtyping into the *algorithmic version*

The problem was that we don't have an algorithm to decide when $S <: T$ or $\Gamma \vdash t : T$

Both sets of rules are not *syntax-directed*

What to do?

1. *Observation*: We don't *need* lots of 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.

Chap 16

Metatheory of Subtyping

Algorithmic Subtyping

Algorithmic Typing

Joins and Meets

Developing an algorithmic subtyping relation

Algorithmic Subtyping

What to do

How do we change the rules deriving $S <: T$ to be *syntax-directed*?

There are lots of ways to derive a given subtyping statement $S <: T$.

The general idea is to *change this system* so that there is *only one way* to derive it.

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

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

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

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

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

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

Step 2: Get rid of reflexivity

Observation: S-REFL is unnecessary.

Lemma 16.1.2: $S <: S$ can be derived for every type S without using S-REFL.

Even simpler subtype relation

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

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

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

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

Step 3: Get rid of transitivity

Observation: S-Trans is unnecessary.

Lemma 16.1.2: If $S <: T$ can be derived, then it can be derived without using S-Trans .

Even simpler subtype relation

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

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

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

"Algorithmic" subtype relation

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

$$\frac{\mapsto T_1 <: S_1 \qquad \mapsto S_2 <: T_2}{\mapsto S_1 \rightarrow S_2 <: T_1 \rightarrow T_2} \qquad (\text{SA-Arrow})$$

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

Soundness and completeness

Theorem[16.1.5]: $S <: T$ iff $\mapsto S <: T$

Terminology:

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

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?

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

1. if $subtype(\mathrm{S}, \mathrm{T}) = true$, then $\mapsto \mathrm{S} <: \mathrm{T}$

   hence, by soundness of the algorithmic rules, $\mathrm{S} <: \mathrm{T}$

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

Q: What's missing?

Decision Procedures

Is our *subtype* function a decision procedure?

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

1. if $subtype(\mathrm{S},\mathrm{T}) = true$, then $\mapsto \mathrm{S} <: \mathrm{T}$

   (hence, by soundness of the algorithmic rules, $\mathrm{S} <: \mathrm{T}$)

1. if $subtype(\mathrm{S},\mathrm{T}) = false$, then not $\mapsto \mathrm{S} <: \mathrm{T}$

   (hence, by completeness of the algorithmic rules, not $\mathrm{S} <: \mathrm{T}$)

Q: What's missing?

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

Decision Procedures

Is our *subtype* function a decision procedure?

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

1. if $subtype(\mathrm{S},\mathrm{T}) = true$, then $\mapsto \mathrm{S} <: \mathrm{T}$

   (hence, by soundness of the algorithmic rules, $\mathrm{S} <: \mathrm{T}$)

1. if $subtype(\mathrm{S},\mathrm{T}) = false$, then not $\mapsto \mathrm{S} <: \mathrm{T}$

   (hence, by completeness of the algorithmic rules, not $\mathrm{S} <: \mathrm{T}$)

Q: What’s missing?

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

Prove it!

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 $u \in R$.

Example:

$$U = \{1, 2, 3\}$$
$$R = \{(1, 2), (2, 3)\}$$

Note that, we are saying nothing about *computability.*

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 $u \in R$.

Example:

$$U = \{1, 2, 3\}$$

$$R = \{(1, 2), (2, 3)\}$$

The function p' whose graph is

{((1, 2), *true*), ((2, 3), *true*)}

is *not* a decision function for R

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 $u \in R$.

Example:

$$U = \{1, 2, 3\}$$

$$R = \{(1, 2), (2, 3)\}$$

The function p'' whose graph is

{((1, 2), *true*), ((2, 3), *true*), ((1, 3), *false*)}

is also *not* a decision function for R

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 $u \in R$.

Example:

$$U = \{1, 2, 3\}$$
$$R = \{(1, 2), (2, 3)\}$$

The function p whose graph is

{ ((1, 2), *true*), ((2, 3), *true*),
((1, 1), *false*), ((1, 3), *false*),
((2, 1), *false*), ((2, 2), *false*),
((3, 1), *false*), ((3, 2), *false*), ((3, 3), *false*)}

is a decision function for R

Decision Procedures (take 2)

We want *a decision procedure* to be a *procedure*.

A *decision procedure* for a relation $R \subseteq U$ is a ***computable*** *total function* p from U to *{true, false}* such that

$$p(u) = true \text{ iff } \mathrm{u} \in R.$$

Example

$$U = \{1, 2, 3\}$$
$$R = \{(1,2), (2,3)\}$$

The function

$$p(x, y) = if \quad x = 2 \; and \; y = 3 \quad then \; true$$
$$else \; if \; x = 1 \; and \; y = 2 \quad then \; true$$
$$else \; false$$

whose graph is

{ ((1, 2), *true*), ((2, 3), *true*),
((1, 1), *false*), ((1, 3), *false*),
((2, 1), *false*), ((2, 2), *false*),
((3, 1), *false*), ((3, 2), *false*), ((3, 3), *false*)}

is a decision procedure for R.

Example

$$U = \{1, 2, 3\}$$
$$R = \{(1, 2), (2, 3)\}$$

The recursively defined *partial function*

$$\begin{aligned} p(x, y) = if\quad & x = 2\ and\ y = 3\ then\ true \\ & else\ if\ x = 1\ and\ y = 2\ then\ true \\ & else\ if\ x = 1\ and\ y = 3\ then\ false \\ & else\ p(x, y) \end{aligned}$$

whose graph is

{ ((1, 2), *true*), ((2, 3), *true*), ((1, 3), *false*)}

is *not* a decision procedure for R.

Subtyping Algorithm

The following *recursively defined total function* is a *decision procedure* for the subtype relation:

subtype(S, T) =

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

else if $\mathrm{S} = \mathrm{S}_1 \longrightarrow \mathrm{S}_2$ and $\mathrm{T} = \mathrm{T}_1 \longrightarrow \mathrm{T}_2$

then $subtype(\mathrm{T}_1, \mathrm{S}_1) \wedge subtype(\mathrm{S}_2, \mathrm{T}_2)$

else if $\mathrm{S} = \{\mathrm{k}_\mathrm{j}\colon\ \mathrm{S}_\mathrm{j}{}^{\mathrm{j}\in 1..\mathrm{m}}\}$ and $\mathrm{T} = \{\mathrm{l}_\mathrm{i}\colon\ \mathrm{T}_\mathrm{i}{}^{\mathrm{i}\in 1..n}\}$

then $\{\mathrm{l}_\mathrm{i}{}^{\mathrm{i}\in 1..\mathrm{n}}\} \subseteq \{\mathrm{k}_\mathrm{j}{}^{\mathrm{j}\in 1..\mathrm{m}}\}$

$\wedge$ for all $i \in 1..n$ there is some $j \in 1..m$ with $\mathrm{k}_\mathrm{j} = \mathrm{l}_\mathrm{i}$ and $subtype(\mathrm{S}_\mathrm{j}, \mathrm{T}_\mathrm{i})$

else *false*.

Subtyping Algorithm

This *recursively defined total function* is a decision procedure for the subtype relation:

subtype(S, T) =

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

else if $\mathrm{S} = \mathrm{S}_1 \longrightarrow \mathrm{S}_2$ and $\mathrm{T} = \mathrm{T}_1 \longrightarrow \mathrm{T}_2$

then $subtype(\mathrm{T}_1, \mathrm{S}_1) \wedge subtype(\mathrm{S}_2, \mathrm{T}_2)$

else if $\mathrm{S} = \{\mathrm{k}_\mathrm{j}\colon\ \mathrm{S}_\mathrm{j}{}^{\mathrm{j}\in 1..\mathrm{m}}\}$ and $\mathrm{T} = \{\mathrm{l}_\mathrm{i}\colon\ \mathrm{T}_\mathrm{i}{}^{\mathrm{i}\in 1..n}\}$

then $\{\mathrm{l}_\mathrm{i}{}^{\mathrm{i}\in 1..\mathrm{n}}\} \subseteq \{\mathrm{k}_\mathrm{j}{}^{\mathrm{j}\in 1..\mathrm{m}}\}$

$\wedge$ for all $i \in 1..n$ there is some $j \in 1..m$ with $\mathrm{k}_\mathrm{j} = \mathrm{l}_\mathrm{i}$ and $subtype(\mathrm{S}_\mathrm{j}, \mathrm{T}_\mathrm{i})$

else *false*.

To show this, we *need to prove* :

1. that it returns $true$ whenever $\mathrm{S} <: \mathrm{T}$, and
2. that it returns either $true$ or $false$ on *all inputs*

[16.1.6 Termination Proposition]

Algorithmic Typing

Algorithmic typing

How do we implement a *type checker* for the lambda-calculus *with subtyping*?

Given a context Γ and a term t, how do we determine its type T, such that $\Gamma \vdash t : T$?

Issue

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

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

Q: where is this rule really needed?

For *applications*, e.g., the term

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

is *not typable* without using subsumption.

Where else??

Nowhere else!

Uses of subsumption rule to help typecheck *applications* are the only interesting ones.

Plan

1. Investigate *how subsumption is used* in typing derivations by *looking at examples* of how it can be "*pushed through*" other rules;
2. Use the intuitions gained from these examples to design a new, algorithmic typing relation that
   - *Omits subsumption;*
   - Compensates for its absence by *enriching the application rule;*
3. *Show that* the *algorithmic typing relation* is essentially equivalent to the original, *declarative one.*

Example (T-ABS)

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

becomes

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

Intuitions

These examples show that ***we do not need T-SUB to "enable" T-ABS*** :

> given any typing derivation, we **can construct a derivation** *with the same conclusion* in which T-SUB *is never used immediately before* $T\text{-}ABS$.

What about $T\text{-}APP$?

We've already observed that T-SUB is required for typechecking some *applications*

Therefore we expect to find that we ***cannot*** play the same game with T-APP as we've done with T-ABS

Let's see why.

Example (T–Sub with T-APP on the left)

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

becomes

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

Example (T–Sub with T-APP on the right)

$$\dfrac{\dfrac{\vdots}{\Gamma \vdash s_1 : T_{11}\to T_{12}} \qquad \dfrac{\dfrac{\vdots}{\Gamma \vdash s_2 : T_2} \qquad \dfrac{\vdots}{T_2 <: T_{11}}}{\Gamma \vdash s_2 : T_{11}}\ (\text{T-Sub})}{\Gamma \vdash s_1\ s_2 : T_{12}}\ (\text{T-App})$$

becomes

$$\dfrac{\boxed{\dfrac{\dfrac{\vdots}{\Gamma \vdash s_1 : T_{11}\to T_{12}} \qquad \dfrac{\dfrac{\vdots}{T_2 <: T_{11}} \qquad \dfrac{}{T_{12} <: T_{12}}\ (\text{S-Refl})}{T_{11}\to T_{12} <: T_2\to T_{12}}\ (\text{S-Arrow})}{\Gamma \vdash s_1 : T_2\to T_{12}}\ (\text{T-Sub})} \qquad \dfrac{\vdots}{\Gamma \vdash s_2 : T_2}}{\Gamma \vdash s_1\ s_2 : T_{12}}\ (\text{T-App})$$

Observations

We've seen that uses of subsumption rule can be "*pushed*" from one of immediately before T-APP's premises to the other, but *cannot be completely eliminated*

Example (nested uses of T-Sub)

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

becomes

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

Summary

What we've learned:

- Uses of the T-Sub rule can be "*pushed down*" through typing derivations until they encounter either
  1. a use of T-App , or
  2. the *root* of the derivation tree.
- In both cases, ***multiple uses of* T-Sub *can be coalesced into a single one***.

This suggests a notion of "*normal form*" for typing derivations, in which there is

- exactly one use of T-Sub before each use of T-App,
- one use of T-Sub at the very end of the derivation,
- no uses of T T-Sub anywhere else.

Algorithmic Typing

The next step is to "build in" the use of subsumption rule in *application rules*, by *changing* the T-App rule to *incorporate a subtyping premise*

$$\frac{\Gamma \vdash t_1 : T_{11}{\rightarrow}T_{12} \qquad \Gamma \vdash t_2 : T_2 \qquad \boxed{\vdash T_2 <: T_{11}}}{\Gamma \vdash t_1\ t_2 : T_{12}}$$

Given any typing derivation, we can now

1. normalize it, to *move all uses of subsumption rule* to either just *before applications* (in the right-hand premise) or *at the very end*
2. replace uses of T-App with T-SUB in the right-hand premise by uses of the extended rule above

This yields a derivation in which there is just *one* use of subsumption, at the very end!

Minimal Types

But... if subsumption is only used at the very end of derivations, then it is actually *not needed* in order to show that *any term is typable*!

It is just used to give *more* types to terms that have already been shown to have a type.

In other words, if we *dropped subsumption completely* (after refining the application rule), we would still be able to give types to exactly the same set of terms — we just would not be able to give as *many types* to some of them.

If we drop subsumption, then the remaining rules will assign a *unique*, *minimal* type to *each typable term*

For purposes of building a typechecking algorithm, this is enough

Final Algorithmic Typing Rules

$$\frac{x{:}T \in \Gamma}{\Gamma \blacktriangleright x : T} \qquad \text{(TA-VAR)}$$

$$\frac{\Gamma, x{:}T_1 \blacktriangleright t_2 : T_2}{\Gamma \blacktriangleright \lambda x{:}T_1.t_2 : T_1 \to T_2} \qquad \text{(TA-ABS)}$$

$$\frac{\Gamma \blacktriangleright t_1 : T_1 \qquad T_1 = T_{11} \to T_{12} \qquad \Gamma \blacktriangleright t_2 : T_2 \qquad \boxed{\blacktriangleright T_2 <: T_{11}}}{\Gamma \blacktriangleright t_1\ t_2 : T_{12}}$$

$$\text{(TA-APP)}$$

$$\frac{\text{for each } i \qquad \Gamma \blacktriangleright t_i : T_i}{\Gamma \blacktriangleright \{l_1{=}t_1 \ldots l_n{=}t_n\} : \{l_1{:}T_1 \ldots l_n{:}T_n\}} \qquad \text{(TA-RCD)}$$

$$\frac{\Gamma \blacktriangleright t_1 : R_1 \qquad R_1 = \{l_1{:}T_1 \ldots l_n{:}T_n\}}{\Gamma \blacktriangleright t_1.l_i : T_i} \qquad \text{(TA-PROJ)}$$

Completeness of the algorithmic rules

Theorem [Minimal Typing]:

If $\Gamma \vdash t : T$, then $\Gamma \mapsto t : S$ for some $S <: T$.

Proof: Induction on *typing derivation*.

N.b.: All the messing around with transforming derivations was just to build intuitions and *decide what algorithmic rules* to write down and *what property* to prove:

the proof itself is *a straightforward induction on typing derivations.*

Meets and Joins

Adding Booleans

Suppose we want to add *booleans* and *conditionals* to the language we have been discussing.

For the declarative presentation of the system, we just add in the appropriate *syntactic forms*, *evaluation rules*, and *typing rules*.

$$\Gamma \vdash \mathtt{true} : \mathtt{Bool} \qquad \text{(T-TRUE)}$$

$$\Gamma \vdash \mathtt{false} : \mathtt{Bool} \qquad \text{(T-FALSE)}$$

$$\frac{\Gamma \vdash \mathtt{t}_1 : \mathtt{Bool} \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T} \qquad \Gamma \vdash \mathtt{t}_3 : \mathtt{T}}{\Gamma \vdash \mathtt{if}\ \mathtt{t}_1\ \mathtt{then}\ \mathtt{t}_2\ \mathtt{else}\ \mathtt{t}_3 : \mathtt{T}} \qquad \text{(T-IF)}$$

A Problem with Conditional Expressions

For the *algorithmic presentation* of the system, however, we encounter a little difficulty.

What is the minimal type of

$if\ true\ then\ \{x = true, y = false\}\ else\ \{x = true, z = true\}$?

The Algorithmic Conditional Rule

More generally, we can use subsumption to give an expression

$\text{if } t_1 \text{ then } t_2 \text{ else } t_3$

any type that is a possible type of both t_2 and t_3.

So the *minimal* type of the *conditional* is the

least common supertype (or *join*) of

the minimal type of t_2 and the minimal type of t_3

$$\frac{\Gamma \mapsto t_1 : \mathtt{Bool} \qquad \Gamma \mapsto t_2 : T_2 \qquad \Gamma \mapsto t_3 : T_3}{\Gamma \mapsto \mathtt{if}\ t_1\ \mathtt{then}\ t_2\ \mathtt{else}\ t_3 : T_2 \vee T_3} \quad \text{(T-If)}$$

Q: Does such a type exist for every T_2 and T_3 ??

Existence of Joins

Theorem: For every pair of types S and T, there is a type J such that

1. $S <: J$
2. $T <: J$
3. If K is a type such that $S <: K$ and $T <: K$, then $J <: K$.

i.e., J is the *smallest type* that is a supertype of both S and T.

How to prove it?

Calculating Joins

$$
\mathtt{S} \vee \mathtt{T} \quad = \quad \begin{cases}
\mathtt{Bool} & \text{if } \mathtt{S} = \mathtt{T} = \mathtt{Bool} \\
\mathtt{M}_1 \rightarrow \mathtt{J}_2 & \text{if } \mathtt{S} = \mathtt{S}_1 \rightarrow \mathtt{S}_2 \quad \mathtt{T} = \mathtt{T}_1 \rightarrow \mathtt{T}_2 \\
 & \quad \mathtt{S}_1 \wedge \mathtt{T}_1 = \mathtt{M}_1 \quad \mathtt{S}_2 \vee \mathtt{T}_2 = \mathtt{J}_2 \\
\{\mathtt{j}_l : \mathtt{J}_l\ ^{l \in 1..q}\} & \text{if } \mathtt{S} = \{\mathtt{k}_j : \mathtt{S}_j\ ^{j \in 1..m}\} \\
 & \quad \mathtt{T} = \{\mathtt{l}_i : \mathtt{T}_i\ ^{i \in 1..n}\} \\
 & \quad \{\mathtt{j}_l\ ^{l \in 1..q}\} = \{\mathtt{k}_j\ ^{j \in 1..m}\} \cap \{\mathtt{l}_i\ ^{i \in 1..n}\} \\
 & \quad \mathtt{S}_j \vee \mathtt{T}_i = \mathtt{J}_l \quad \text{for each } \mathtt{j}_l = \mathtt{k}_j = \mathtt{l}_i \\
\mathtt{Top} & \text{otherwise}
\end{cases}
$$

Examples

What are the joins of the following pairs of types?

1. $\{x: Bool, y: Bool\}$ and $\{y: Bool, z: Bool\}$?
2. $\{x: Bool\}$ and $\{y: Bool\}$?
3. $\{x: \{a: Bool, b: Bool\}\}$ and $\{x: \{b: Bool, c: Bool\}, y: Bool\}$?
4. $\{\}$ and $Bool$?
5. $\{x: \{\}\}$ and $\{x: Bool\}$?
6. $Top \longrightarrow \{x: Bool\}$ and $Top \longrightarrow \{y: Bool\}$?
7. $\{x: Bool\} \longrightarrow Top$ and $\{y: Bool\} \longrightarrow Top$?

Meets

To calculate joins of arrow types, we also need to be able to calculate meets (greatest lower bounds)!

Unlike joins, meets *do not necessarily exist*.

E.g., $\mathrm{Bool} \longrightarrow \mathrm{Bool}$ and $\{\}$ have *no common subtypes*, so they certainly don't have a greatest one!

Existence of Meets

Theorem: For every pair of types S and T, we say that a type M is a meet of S and T, written $S \wedge T = M$ if

1. $M <: S$
2. $M <: T$
3. If O is a type such that $O <: S$ and $O <: T$, then $O <: M$.

i.e., M (when it exists) is the *largest type* that is a subtype of both S and T.

Jargon: In the simply typed lambda calculus with subtyping, records, and booleans ...

- The subtype relation *has joins*
- The subtype relation *has bounded meets*

Calculating Meets

$$
S \wedge T \quad = \quad
\begin{cases}
S & \text{if } T = Top \\
T & \text{if } S = Top \\
Bool & \text{if } S = T = Bool \\
J_1 \rightarrow M_2 & \text{if } S = S_1 \rightarrow S_2 \quad T = T_1 \rightarrow T_2 \\
 & \quad S_1 \vee T_1 = J_1 \quad S_2 \wedge T_2 = M_2 \\
\{m_l : M_l \ ^{l \in 1..q}\} & \text{if } S = \{k_j : S_j \ ^{j \in 1..m}\} \\
 & \quad T = \{l_i : T_i \ ^{i \in 1..n}\} \\
 & \quad \{m_l \ ^{l \in 1..q}\} = \{k_j \ ^{j \in 1..m}\} \cup \{l_i \ ^{i \in 1..n}\} \\
 & \quad S_j \wedge T_i = M_l \qquad \text{for each } m_l = k_j = l_i \\
 & \quad M_l = S_j \qquad \text{if } m_l = k_j \text{ occurs only in } S \\
 & \quad M_l = T_i \qquad \text{if } m_l = l_i \text{ occurs only in } T \\
fail & \text{otherwise}
\end{cases}
$$

Examples

What are the meets of the following pairs of types?

1. $\{x\text{: Bool}, y\text{: Bool}\}$ and $\{y\text{: Bool}, z\text{: Bool}\}$?
2. $\{x\text{: Bool}\}$ and $\{y\text{: Bool}\}$?
3. $\{x\text{: }\{a\text{: Bool}, b\text{: Bool}\}\}$ and $\{x\text{: }\{b\text{: Bool}, c\text{: Bool}\}, y\text{: Bool}\}$?
4. $\{\}$ and Bool?
5. $\{x\text{: }\{\}\}$ and $\{x\text{: Bool}\}$?
6. $\text{Top} \longrightarrow \{x\text{: Bool}\}$ and $\text{Top} \longrightarrow \{y\text{: Bool}\}$?
7. $\{x\text{: Bool}\} \longrightarrow \text{Top}$ and $\{y\text{: Bool}\} \longrightarrow \text{Top}$?

Homework☺

- Read and digest chapter 16 & 17
- HW: 16.1.2;   16.2.6;   16. 4.1