编程语言的设计原理
Design Principles of Programming Languages

Haiyan Zhao, Di Wang

赵海燕，王迪

Peking University, Spring Term 2024

Issues in Subtyping

Typing with Subsumption

Principle of safe substitution:

– *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.,

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

Subtype Relation: General rules

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

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

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

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

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.

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

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

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 *"sub-goals"* from the sub-expressions 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 the system is extended 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)

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

2. Worse yet, the new rule T-SUB *itself is not syntax directed*: the ***inputs*** to ***the left-hand sub-goal*** *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?

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*

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

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

Lemma 16.1.1: If **S <: T** is derivable from the subtyping rules including **S-RcdDepth**, **S-Rcd-Width**, and **S-Rcd-Perm** (but not **S-Rcd**), then it can also be derived using **S-Rcd** (and not **-RcdDepth**, **S-Rcd-Width**, or **S-Rcd-Perm**), and vice versa.

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

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

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

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

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

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

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

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

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

"Algorithmic" subtype relation

Definition: The *algorithmic subtyping relation* is the least relation on types closed under the following 3 rules

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

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

$$\frac{\{l_i\ ^{i \in 1..n}\} \subseteq \{k_j\ ^{j \in 1..m}\} \qquad \text{for each } k_j = l_i,\ \mapsto S_j <: T_i}{\mapsto \{k_j : S_j\ ^{j \in 1..m}\} <: \{l_i : T_i\ ^{i \in 1..n}\}} \qquad \text{(SA-RCD)}$$

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*)

Subtyping Algorithm

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*.

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, $\mathrm{S} <: \mathrm{T}$

2. 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:

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

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

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 $\mathrm{S} = \mathrm{S}_1 \rightarrow \mathrm{S}_2$ and $\mathrm{T} = \mathrm{T}_1 \rightarrow \mathrm{T}_2$

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

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

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 $T = Top$ then *true*

else if $S = S_1 \rightarrow S_2$ and $T = T_1 \rightarrow T_2$

then $subtype(T_1, S_1) \wedge subtype(S_2, T_2)$

else if $S = \{k_j: S_j{}^{j \in 1..m}\}$ and $T = \{l_i: T_i{}^{i \in 1..n}\}$

then $\{l_i{}^{i \in 1..n}\} \subseteq \{k_j{}^{j \in 1..m}\}$

$\wedge$ for all $i \in 1..n$ there is some $j \in 1..m$ with $k_j = l_i$ and $subtype(S_j, T_i)$

else *false*.

To show this, we *need to prove* :

1. that it returns $true$ whenever $S <: T$, 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*

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

Q: where is this rule really needed?

For *applications*, e.g., the term $(\lambda r{:}\{x{:}\,Nat\}.\,r.x)\{x = 0, y = 1\}$ is *not typable* without using subsumption.

Where else??

Nowhere else!

Uses of subsumption rule to help typecheck *applications* are the only interesting ones (where subsumption plays a crucial role in typing)

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)

becomes

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

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

Intuitions

These examples show that ***we do not need to*** T-SUB ***"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-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)

becomes

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

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

Example (T—Sub with T-App on the right)

becomes

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

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

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)

becomes

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

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

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*

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

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

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

$$\frac{\Gamma, x:T_1 \blacktriangleright t_2 : T_2}{\Gamma \blacktriangleright \lambda x:T_1.t_2 : T_1 \rightarrow T_2} \quad \text{(TA-Abs)}$$

$$\frac{\Gamma \blacktriangleright t_1 : T_1 \qquad T_1 = T_{11} \rightarrow T_{12} \qquad \Gamma \blacktriangleright t_2 : T_2 \qquad \blacktriangleright T_2 <: T_{11}}{\Gamma \blacktriangleright t_1\ t_2 : T_{12}} \quad \text{(TA-App)}$$

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

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

Completeness of the algorithmic rules

Theorem [Minimal Typing]:

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

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*.

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

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

$$\frac{\Gamma \vdash t_1 : \texttt{Bool} \qquad \Gamma \vdash t_2 : T \qquad \Gamma \vdash t_3 : T}{\Gamma \vdash \texttt{if } t_1 \texttt{ then } t_2 \texttt{ else } t_3 : T} \qquad \text{(T-IF)}$$

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

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

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

$$
S \vee T \quad = \quad \begin{cases}
\texttt{Bool} & \text{if } S = T = \texttt{Bool} \\
M_1 \rightarrow J_2 & \text{if } S = S_1 \rightarrow S_2 \quad T = T_1 \rightarrow T_2 \\
 & \quad S_1 \wedge T_1 = M_1 \quad S_2 \vee T_2 = J_2 \\
\{j_l : J_l \ ^{l \in 1..q}\} & \text{if } S = \{k_j : S_j \ ^{j \in 1..m}\} \\
 & \quad T = \{l_i : T_i \ ^{i \in 1..n}\} \\
 & \quad \{j_l \ ^{l \in 1..q}\} = \{k_j \ ^{j \in 1..m}\} \cap \{l_i \ ^{i \in 1..n}\} \\
 & \quad S_j \vee T_i = J_l \quad \text{for each } j_l = k_j = l_i \\
\texttt{Top} & \text{otherwise}
\end{cases}
$$

Examples

What are the joins of the following pairs of types?

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

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., $\text{Bool} \longrightarrow \text{Bool}$ 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

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

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. $\{x: \{a: \text{Bool}, b: \text{Bool}\}\}$ and $\{x: \{b: \text{Bool}, c: \text{Bool}\}, y: \text{Bool}\}$?
4. $\{\}$ and Bool?
5. $\{x: \{\}\}$ 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