Four Forms of Polymorphism
SIGPL Summer School 2019

Giuseppe Castagna

CNRS
Outline of the course

- Background and Motivations
  Polymorphism - Motivating Examples - A Refresher Course on Operational Semantics

- Subtyping polymorphism
  Simple Types - Recursive Types - Bibliography

- Parametric polymorphism
  Introduction - Hindley-Milner System - Inference algorithm

- Ad-Hoc polymorphism

- Gradual Typing (dynamic type polymorphism)
  Main ideas - Formal system - Algorithmic Aspects - Criteria for Gradual Typing - Implementation issues - References
Background and Motivations
Outline

1. Polymorphism
2. Motivating Examples
3. A Refresher Course on Operational Semantics
Outline

1. Polymorphism
2. Motivating Examples
3. A Refresher Course on Operational Semantics
What is polymorphism?

Merriam-Webster Dictionary

The quality or state of existing in or assuming different forms

In computing: the capability of a programming entity to act as being of different types.

There exists several polymorphic programming entities:
- polymorphic functions (e.g., a function of type \( \texttt{int} \rightarrow \texttt{int} \) and of type \( \texttt{bool} \rightarrow \texttt{bool} \))
- polymorphic data structures (e.g., a list whose elements are of any possible type)
- polymorphic classes (e.g. a class whose instances are stack of \( \texttt{int} \) and \( \texttt{bool} \))
- polymorphic operators (e.g., the symbol \( + \) to denote arithmetic sum and \( \texttt{string} \) concatenation...)

In this course I focus on functions.
What is polymorphism?

Merriam-Webster Dictionary

The quality or state of existing in or assuming different forms

In computing: the capability of a programming entity to act as of being of different types.
What is polymorphism?

Merriam-Webster Dictionary
The quality or state of existing in or assuming different forms

In computing: the capability of a programming entity to act as of being of different types.
There exists several polymorphic programming entities:
- polymorphic functions (e.g., a function of type `int → int` and of type `bool → bool`)
- polymorphic data structures (e.g., a list whose elements are of any possible type)
- polymorphic classes (e.g. a class whose instances are stack of `int` and stacks of `bool`)
- polymorphic operators (e.g., the symbol `+` to denote arithmetic sum and string concatenation)
- ...

In this course I focus on functions.

G. Castagna (CNRS)
What is polymorphism?

Merriam-Webster Dictionary
The quality or state of existing in or assuming different forms

In computing: the capability of a programming entity to act as of being of different types.

There exists several polymorphic programming entities:

- **polymorphic functions** (e.g., a function of type `int → int` and of type `bool → bool`)
- polymorphic data structures (e.g., a list whose elements are of any possible type)
- polymorphic classes (e.g., a class whose instances are stack of `int` and stacks of `bool`)
- polymorphic operators (e.g., the symbol `+` to denote arithmetic sum and string concatenation)

...
Polymorphic functions

Functions that can be applied to arguments of different types

Four forms of polymorphism:
1. parametric,
2. subtyping,
3. ad-hoc,
4. dynamic.

GOAL: How to define sound type system for polymorphic functions

Sound = all expressions that pass type-checking will never reduce to stuck terms such as 3(true).
Polymorphic functions

Functions that can be applied to arguments of different types

GOAL

How to define sound type system for polymorphic functions

Sound = all expressions that pass type-checking will never reduce to stuck terms such as \(3(\text{true})\)
Polymorphic functions

Functions that can be applied to arguments of different types

GOAL

How to define sound type system for polymorphic functions

Sound = all expressions that pass type-checking will never reduce to stuck terms such as $3(\text{true})$

Four forms of polymorphism:

1. parametric,
2. subtyping,
3. ad-hoc,
4. dynamic
Four kinds of polymorphism

1. **Parametric polymorphism:**
   Functions that work with arguments of any type.
Four kinds of polymorphism

1. **Parametric polymorphism:**
   Functions that work with arguments of any type.
   They do not inspect “parametric” arguments, they just:
   - either ignore them
   - or pass them to other polymorphic functions
   - or return them in the result

2. **Subtyping polymorphism:**
   Functions that work with arguments having certain properties:
   They use the known properties of the arguments

3. **Ad-hoc polymorphism (a.k.a. overloading):**
   Functions that work with arguments belonging to a specific (finite) set of different types
   They execute different code for each type of the argument

4. **Dynamic/Unknown type:**
   Functions that make no assumption about the type of some specific arguments
   They delay the check to the type of these arguments at run-time
Four kinds of polymorphism

1. **Parametric polymorphism:**
   Functions that work with arguments of any type.
   They do not inspect “parametric” arguments, they just:
   - either ignore them
   - or pass them to other polymorphic functions
   - or return them in the result

2. **Subtyping polymorphism:**
   Functions that work with arguments having certain properties:
Four kinds of polymorphism

1. **Parametric polymorphism:**
   Functions that work with arguments of any type. They do not inspect “parametric” arguments, they just:
   - either ignore them
   - or pass them to other polymorphic functions
   - or return them in the result

2. **Subtyping polymorphism:**
   Functions that work with arguments having certain properties:
   They use the known properties of the arguments
Four kinds of polymorphism

1. **Parametric polymorphism:**
   Functions that work with arguments of any type.
   They do not inspect “parametric” arguments, they just:
   - either ignore them
   - or pass them to other polymorphic functions
   - or return them in the result

2. **Subtyping polymorphism:**
   Functions that work with arguments having certain properties:
   They use the known properties of the arguments

3. **Ad-hoc polymorphism (a.k.a. overloading):**
   Functions that work with arguments belonging to a specific (finite) set of different types
Four kinds of polymorphism

1. **Parametric polymorphism:**
   Functions that work with arguments of any type.
   They do not inspect “parametric” arguments, they just:
   - either ignore them
   - or pass them to other polymorphic functions
   - or return them in the result

2. **Subtyping polymorphism:**
   Functions that work with arguments having certain properties:
   They use the known properties of the arguments

3. **Ad-hoc polymorphism (a.k.a. overloading):**
   Functions that work with arguments belonging to a specific (finite) set of different types
   They execute different code for each type of the argument
Four kinds of polymorphism

1. **Parametric polymorphism:**
   Functions that work with arguments of any type. They do not inspect “parametric” arguments, they just:
   - either ignore them
   - or pass them to other polymorphic functions
   - or return them in the result

2. **Subtyping polymorphism:**
   Functions that work with arguments having certain properties:
   They use the known properties of the arguments

3. **Ad-hoc polymorphism (a.k.a. overloading):**
   Functions that work with arguments belonging to a specific (finite) set of different types
   They execute different code for each type of the argument

4. **Dynamic/Unknown type:**
   Functions that make no assumption about the type of some specific arguments
Four kinds of polymorphism

1. **Parametric polymorphism:**
   Functions that work with arguments of any type. They do not inspect “parametric” arguments, they just:
   - either ignore them
   - or pass them to other polymorphic functions
   - or return them in the result

2. **Subtyping polymorphism:**
   Functions that work with arguments having certain properties:
   They use the known properties of the arguments

3. **Ad-hoc polymorphism (a.k.a. overloading):**
   Functions that work with arguments belonging to a specific (finite) set of different types
   They execute different code for each type of the argument

4. **Dynamic/Unknow type:**
   Functions that make no assumption about the type of some specific arguments
   They delay the check to the type of these arguments at run-time
Outline

1. Polymorphism
2. Motivating Examples
3. A Refresher Course on Operational Semantics
1. Parametric polymorphism

Functions that work with arguments of any type.

They do not inspect “parametric” arguments, they just:

- either ignore them
- or pass them to other polymorphic functions
- or return them in the result

```javascript
function first (x , y) {
    return x;
}
```

It can be applied to pairs of type $S \times T \rightarrow S$ and returns a result of type $S$, whatever types $S$ and $T$ are.
Functions that work with arguments of any type.

They do not inspect “parametric” arguments, they just:

- either ignore them
- or pass them to other polymorphic functions
- or return them in the result

function first (x , y) {
  return x;
}

It can be applied to pairs of type $S \times T \rightarrow S$ and returns a result of type $S$, whatever types $S$ and $T$ are.

Intuition

Add type variables and quantify them universally:

$$\forall \alpha, \beta . \alpha \times \beta \rightarrow \alpha$$
Functions that work with arguments of with certain properties: They use the known properties of the arguments

```javascript
function size (x) {
    return x.length;
}
```

It can be applied to objects with the property `length` and return (in general) an integer.
2. Subtyping polymorphism

**Functions that work with arguments of with certain properties:** They use the known properties of the arguments

```javascript
function size(x) {
    return x.length;
}
```

It can be applied to objects with the property `length` and return (in general) an integer.

**Intuition**

Define an order relation on types and accept arguments of any subtype

```
{ length: number } \rightarrow number
```

Accepts arguments of any type $T \leq \{ length: number \}$

(e.g. $\{ length: number, concat: string \rightarrow string \}$)
function size (x) {
    return x.length;
}

Subtyping + Parametric

Possibility two combine the two form of polymorphism

∀α. { length : α } → α
function size (x) {
    return x.length;
}

Subtyping + Parametric

Possibility two combine the two form of polymorphism

$$\forall \alpha. \{ \text{length} : \alpha \} \rightarrow \alpha$$

function size (x) {
    if (x.length > 4) { x = setCharAt(str,4,’a’) }
    return x
}

Bounded parametric

$$\forall \alpha \leq \{ \text{length} : \text{number} \} . \alpha \rightarrow \alpha$$
3. *Ad hoc* polymorphism

Functions for arguments in a specific (finite) set of different types
They execute different code for each type of the argument

```javascript
function double (x) {
    (typeof(x) === "number") ? 2*x : x.concat(x)
}
```

If applied to an integer returns an integer, if applied to a string returns a string
3. *Ad hoc* polymorphism

**Functions for arguments in a specific (finite) set of different types**

They execute different code for each type of the argument

```javascript
function double(x) {
    (typeof(x) === "number") ? 2*x : x.concat(x)
}
```

If applied to an integer returns an integer, if applied to a string returns a string

**Use set-theoretic types**
3. *Ad hoc* polymorphism

**Functions for arguments in a specific (finite) set of different types**
They execute different code for each type of the argument

```javascript
function double (x) {
  (typeof(x) === "number") ? 2*x : x.concat(x)
}
```

If applied to an integer returns an integer, if applied to a string returns a string

**Use set-theoretic types**

- Naive solution: union types
  
  $$(\text{number}|\text{string}) \rightarrow (\text{number}|\text{string})$$
**3. Ad hoc polymorphism**

**Functions for arguments in a specific (finite) set of different types**

They execute different code for each type of the argument

```javascript
function double (x) {
    (typeof(x) === "number") ? 2*x : x.concat(x)
}
```

If applied to an integer returns an integer, if applied to a string returns a string

**Use set-theoretic types**

- Naive solution: union types

  
  $(\text{number}|\text{string})\rightarrow(\text{number}|\text{string})$
3. *Ad hoc* polymorphism

**Functions for arguments in a specific (finite) set of different types**

They execute different code for each type of the argument

```javascript
function double (x) {
  (typeof(x) === "number") ? 2*x : x.concat(x)
}
```

If applied to an integer returns an integer, if applied to a string returns a string

**Use set-theoretic types**

- Naive solution: union types
  
  \[(\text{number} | \text{string}) \rightarrow (\text{number} | \text{string})\]

- Better solution: intersection types
  
  \[(\text{number} \rightarrow \text{number}) \& (\text{string} \rightarrow \text{string})\]
3. *Ad hoc* polymorphism

**Functions for arguments in a specific (finite) set of different types**

They execute different code for each type of the argument

```javascript
function double (x) {
  (typeof(x) === "number") ? 2*x : x.concat(x)
}
```

If applied to an integer returns an integer, if applied to a string returns a string

**Use set-theoretic types**

- Naive solution: union types
  
  
  ```
  (number|string) → (number|string)
  ```

- Better solution: intersection types
  
  ```
  (number→number) & (string→string)
  ```

needs some form of occurrence typing
function double (x) {
  (typeof(x) === "number") ? 2*x : x.concat(x)
}

Set-theoretic + Subtyping

( number→number ) &
( (not(number) & {concat: string→string}) → string )

Actually, set-theoretic types are defined by subtyping
```javascript
function double (x) {
    (typeof(x) === "number") ? 2*x : x.concat(x)
}
```

Set-theoretic + Subtyping

```plaintext
(number → number) &
((not(number) & \{concat: string → string\}) → string)
```

Actually, set-theoretic types are defined by subtyping

Set-theoretic + Parametric

```plaintext
∀\alpha, \beta. (number → number) &
((\alpha & not(number) & \{concat: \alpha → \beta\}) → \beta)
```
function double (x) {
    (typeof(x) === "number") ? 2*x : x.concat(x)
}

Set-theoretic + Subtyping

( number→number ) &
( (not(number) & {concat: string→string}) → string )

Actually, set-theoretic types are defined by subtyping

Set-theoretic + Parametric

∀α,β. ( number→number ) &
( (α & not(number) & {concat: α→β}) ) → β)

a sophisticated way to write bounded polymorphism and recursive types:

∀β, ∀(γ ≤ not(number) & μX.{concat: X→β}).
( number→number ) & ( γ→β )
4. Dynamic types

Functions that *for some specific arguments* delay the check of types at run-time

```javascript
function double (x) {
    ( typeof(x) === "number" ) ? 2*x : x.concat(x)
}
```

 Cannot give a type to x that works with both 2*x and x.concat(x)

Solution

Add an unknown/type "???

Develop a type theory for "???

No solution for ???

for some execution

⇒ statically reject

No problem for any solution for ???

⇒ statically accept, do nothing

For each possible execution there exists some solution for ???

⇒ statically accept and add run-time checks
4. Dynamic types

Functions that *for some specific arguments* delay the check of types at run-time

```javascript
function double (x) {
    (<some twisted condition>) ? 2*x : x.concat(x)
}
```
4. Dynamic types

Functions that *for some specific arguments* delay the check of types at run-time

```javascript
function double (x) {
    (<some twisted condition>) ? 2*x : x.concat(x)
}
```

Cannot give a type to `x` that works with both `2*x` and `x.concat(x)`
4. Dynamic types

Functions that *for some specific arguments* delay the check of types at run-time

```javascript
function double (x : ?) {
    (/<some twisted condition/>)? 2*x : x.concat(x)
}
```

Cannot give a type to `x` that works with both `2*x` and `x.concat(x)`

Solution

Add an unknown/type "?"
4. Dynamic types

Functions that *for some specific arguments* delay the check of types at run-time

```javascript
function double (x : ?) {
    (<some twisted condition>) ? 2*x : x.concat(x)
}
```

Cannot give a type to `x` that works with both `2*x` and `x.concat(x)`

**Solution**

Add an unknown/type “?”

**Develop a type theory for “?” such that:**

- No solution for `?` for some execution ⇒ statically reject
- No problem for any solution for `?` ⇒ statically accept, do nothing
- For each possible execution there exists some solution for `?` ⇒ statically accept and add run-time checks
Reject at compile time:

```javascript
function wrong (x : ?) {
    return (2*x + x(2));  //cannot be a number and a function
}
```
Reject at compile time:

```javascript
function wrong (x : ?) {
    return (2*x + x(2)); //cannot be a number and a function
}
```

Accept as is:

```javascript
function ok (x : ?) {
    if (typeof(x) === "number") { return 42 } else { return x }
}
```

Intuitively the function has type: `? → (number | ?)`
Reject at compile time:

```javascript
function wrong (x : ?) {
    return (2*x + x(2)); //cannot be a number and a function
}
```

Accept as is:

```javascript
function ok (x : ?) {
    if (typeof(x) === "number") { return 42 } else { return x }
}
```

Intuitively the function has type: \( ? \rightarrow (\text{number} | ?) \)

Accept and insert checks:

```javascript
function double (x : ?) {
    (<condition>) ? 2*x : x.concat(x)
}
```

Compile as

```javascript
function double (x : ?) {
    (<condition>) ? 2*(x<number>) : (x<string>).concat(x<string>)
}
```
Combined usage: all 4 together! (OCaml style)

```ocaml
let mymap (condition) (f) (x : ?) =
  if condition then Array.map f x else List.map f x
```
Combined usage: all 4 together! (OCaml style)

```ocaml
let mymap (condition) (f) (x : ?) =  
  if condition then Array.map f x else List.map f x
```

Type: `bool → (α → β) → ? → ?`

Compiled as:

```ocaml
let mymap (condition) (f) (x : (α array | α list) & ?) =  
  if condition then Array.map f (x ⟨α array⟩) else List.map f (x ⟨α list⟩)
```

Cutting edge research: Gradual typing, a new perspective, POPL 19
Combined usage: all 4 together! (OCaml style)

```ocaml
let mymap (condition) (f) (x : ?) =  
    if condition then Array.map f x else List.map f x
```

**Type:** `bool → (α → β) → ? → ?`

- `x` can be bound to anything (though only `α_list` or `α_array` work)
- no information on the type of the result (though only `β_list` or `β_array` are possible)

```ocaml
let mymap (condition) (f) (x : (α array | α list) & ?) =  
    if condition then Array.map f x else List.map f x
```

**Type:** `bool → (α → β) → ((α array | α list) & ?) → (β array | β list)`
Combined usage: all 4 together! (OCaml style)

let mymap (condition) (f) (x : ?) =  
    if condition then Array.map f x else List.map f x

Type: bool → (α → β) → ? → ?

- x can be bound to anything (though only α list or α array work)
- no information on the type of the result (though only β list or β array are possible)

let mymap (condition) (f) (x : (α array | α list) & ?) =  
    if condition then Array.map f x else List.map f x

Type: bool → (α → β) → ( (α array | α list) & ? ) → (β array | β list)

Compiled as:

let mymap (condition) (f) (x : (α array | α list) & ?) =  
    if condition then Array.map f (x⟨α array⟩)  
    else List.map f (x⟨α list⟩)
let mymap (condition) (f) (x : ?) =
  if condition then Array.map f x else List.map f x

Type: bool → (α → β) → ? → ?
- x can be bound to anything (though only α list or α array work)
- no information on the type of the result (though only β list or β array are possible)

let mymap (condition) (f) (x : (α array | α list) & ?) =
  if condition then Array.map f x else List.map f x

Type: bool → (α → β) → ((α array | α list) & ?) → (β array | β list)

Compiled as:
let mymap (condition) (f) (x : (α array | α list) & ?) =
  if condition then Array.map f (x⟨α array⟩)
  else List.map f (x⟨α list⟩)

**Cutting edge research:** *Gradual typing, a new perspective*, POPL 19
1 Polymorphism

2 Motivating Examples

3 A Refresher Course on Operational Semantics
Syntax and small-step semantics

**Syntax**

Terms $a, b ::= N \quad$ Numeric constant

<table>
<thead>
<tr>
<th>$x$ \quad Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>$ab$ \quad Application</td>
</tr>
<tr>
<td>$\lambda x.a$ \quad Abstraction</td>
</tr>
</tbody>
</table>

Values $v ::= \lambda x.a \mid N$
Syntax and small-step semantics

Syntax

Terms  \( a, b \) ::= \( N \) \hspace{1em} \text{Numeric constant} \\
| \hspace{1em} x \hspace{1em} \text{Variable} \\
| \hspace{1em} ab \hspace{1em} \text{Application} \\
| \hspace{1em} \lambda x.a \hspace{1em} \text{Abstraction} \\

Values  \( v \) ::= \lambda x.a \mid N

Small step semantics for strict functional languages

Evaluation Contexts  \( E \) ::= [ ] \mid E a \mid v E

\( \text{BETA}_v (\lambda x.a) v \rightarrow a[v/x] \)

\( \frac{a \rightarrow b}{E[a] \rightarrow E[b]} \)
<table>
<thead>
<tr>
<th>Characteristics of the reduction strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Weak reduction:</strong> We cannot reduce under ( \lambda )-abstractions;</td>
</tr>
<tr>
<td><strong>Call-by-value:</strong> In an application ((\lambda x. a) b), the argument (b) must be fully reduced to a value before (\beta)-reduction can take place.</td>
</tr>
<tr>
<td><strong>Left-most reduction:</strong> In an application (ab), we must reduce (a) to a value first before we can start reducing (b).</td>
</tr>
<tr>
<td><strong>Deterministic:</strong> For every term (a), there is at most one (b) such that (a \rightarrow b).</td>
</tr>
</tbody>
</table>
Strategy and big-step semantics

Characteristics of the reduction strategy

**Weak reduction:** We cannot reduce under \( \lambda \)-abstractions;

**Call-by-value:** In an application \((\lambda x. a) \ b\), the argument \( b \) must be fully reduced to a value before \( \beta \)-reduction can take place.

**Left-most reduction:** In an application \( a \ b \), we must reduce \( a \) to a value first before we can start reducing \( b \).

**Deterministic:** For every term \( a \), there is at most one \( b \) such that \( a \rightarrow b \).

Big step semantics for strict functional languages

\[
\begin{align*}
N &\Rightarrow N \\
\lambda x. a &\Rightarrow \lambda x. a \\
a &\Rightarrow \lambda x. c & b &\Rightarrow v_0 & c[v_0/x] &\Rightarrow v \\
abla b &\Rightarrow v
\end{align*}
\]
The big step semantics induces an efficient implementation

type term =
  Const of int | Var of string | Lam of string * term | App of term * term

exception Error

let rec subst x v = function (* assumes v is closed *)
  | Const n -> Const n
  | Var y -> if x = y then v else Var y
  | Lam(y, b) -> if x = y then Lam(y, b) else Lam(y, subst x v b)
  | App(b, c) -> App(subst x v b, subst x v c)

let rec eval = function
  | Const n -> Const n
  | Var x -> raise Error
  | Lam(x, a) -> Lam(x, a)
  | App(a, b) ->
    match eval a with
    | Lam(x, c) -> let v = eval b in eval (subst x v c)
    | _ -> raise Error
Exercises

1. Define the small-step and big-step semantics for the call-by-name.
2. Deduce from the latter the interpreter.
3. Use the technique introduced for the type \( 'a \) delayed earlier in the course to implement an interpreter with lazy evaluation.
Improving implementation

Environments

- Implementing textual substitution $a[x/v]$ is *inefficient*. This is why compilers and interpreters *do not* implement it.
- Alternative: record the binding $x \mapsto v$ in an *environment* $e$

$$
\begin{align*}
e(x) &= v \\
e \vdash x & \Rightarrow v
\end{align*}
\quad
\begin{align*}
e \vdash N & \Rightarrow N \\
e \vdash \lambda x.a & \Rightarrow \lambda x.a
\end{align*}
\quad
\begin{align*}
e \vdash a & \Rightarrow \lambda x.c \\
e \vdash b & \Rightarrow v_0 \\
e; x & \mapsto v_0 \vdash c \Rightarrow v
\end{align*}
\quad
\begin{align*}
e \vdash ab & \Rightarrow v
\end{align*}

Giving up substitutions in favor of environments does not come for free

Lexical scoping requires careful handling of environments

```latex
let x = 1 in
let f = \lambda y.(x+1) in
let x = "foo" in
f 2
```

In the environment used to evaluate $f 2$ the variable $x$ is bound to 1.
Improving implementation

Environments

Implementing textual substitution $a[x/v]$ is *inefficient*. This is why compilers and interpreters *do not* implement it.

Alternative: record the binding $x \mapsto v$ in an *environment* $e$

\[
\frac{e(x) = v}{e \vdash x \Rightarrow v} \quad \frac{e \vdash N \Rightarrow N}{e \vdash \lambda x.a \Rightarrow \lambda x.a}
\]

\[
\frac{e \vdash a \Rightarrow \lambda x.c \quad e \vdash b \Rightarrow v \circ e; x \mapsto v \circ e \vdash c \Rightarrow v}{e \vdash ab \Rightarrow v}
\]

Giving up substitutions in favor of environments does not come for free
Implementing textual substitution $a[x/v]$ is *inefficient*. This is why compilers and interpreters *do not* implement it.

**Alternative:** record the binding $x \mapsto v$ in an *environment* $e$

\[
\begin{align*}
  e(x) &= v \\
  e \vdash x \Rightarrow v \\
  e \vdash N \Rightarrow N \\
  e \vdash \lambda x.a \Rightarrow \lambda x.a \\
  e \vdash a \Rightarrow \lambda x.c \\
  e \vdash b \Rightarrow v \circ e; x \mapsto v \circ e \vdash c \Rightarrow v \\
  e \vdash a b \Rightarrow v
\end{align*}
\]

Giving up substitutions in favor of environments does not come for free

**Lexical scoping** requires careful handling of environments

```
let x = 1 in
let f = \ y . ( x + 1 ) in
let x = "foo" in
f 2
```

In the environment used to evaluate $f \ 2$ the variable $x$ is bound to 1.
Exercise

Try to evaluate

```
let x = 1 in
let f = \y.(x+1) in
let x = "foo" in
f 2
```

by the big-step semantics in the previous slide,

where `let x = a in b` is syntactic sugar for `(\x.b)a`

*let us outline it together*
Function closures

To implement *lexical scoping in the presence of environments*, function abstractions $\lambda x. a$ must not evaluate to themselves, but to a function *closure*: a pair $(\lambda x. a)[e]$ (ie, the function and the *environment of its definition*).

**Big step semantics with environments and closures**

Values: $v ::= N \mid (\lambda x. a)[e]$

Environments: $e ::= x_1 \mapsto v_1 ; \ldots ; x_n \mapsto v_n$

$e(x) = v \quad \frac{e \vdash N \Rightarrow N}{e \vdash x \Rightarrow v}$

$e \vdash \lambda x. a \Rightarrow (\lambda x. a)[e]$

$e \vdash a \Rightarrow (\lambda x. c)[e_\circ] \quad e \vdash b \Rightarrow v_\circ \quad e_\circ ; x \mapsto v_\circ \vdash c \Rightarrow v$

$e \vdash ab \Rightarrow v$
De Bruijn indexes

Identify variable not by names but by the number $n$ of $\lambda$'s that separate the variable from its binder in the syntax tree.

$$\lambda x. (\lambda y. y x) x \ \text{is} \ \lambda. (\lambda. 0 1) 0$$

$n$ is the variable bound by the $n$-th enclosing $\lambda$. Environments become sequences of values, the $n$-th value of the sequence being the value of variable $n-1$.

Terms

$$a, b ::= N \mid n \mid \lambda. a \mid ab$$

Values

$$v ::= N \mid (\lambda. a)[e]$$

Environments

$$e ::= v_0; v_1; \ldots; v_n$$

$$e \vdash N \Rightarrow N \quad e \vdash \lambda. a \Rightarrow (\lambda. a)[e]$$

$$e \vdash a \Rightarrow (\lambda. c)[e_\circ] \quad e \vdash b \Rightarrow v_\circ \quad v_\circ ; e_\circ \vdash c \Rightarrow v$$

$$e \vdash ab \Rightarrow v$$
The canonical, efficient interpreter

```ocaml
# type term = Const of int | Var of int | Lam of term | App of term * term
and value = Vint of int | Vclos of term * environment
and environment = value list
(* use Vec instead *)

# exception Error

# let rec eval e a =
match a with
| Const n -> Vint n
| Var n -> List.nth e n
| Lam a -> Vclos(Lam a, e)
| App(a, b) ->
  match eval e a with
  | Vclos(Lam c, e') ->
    let v = eval e b in
    eval (v :: e') c
  | _ -> raise Error

# eval [] (App ( Lam (Var 0), Const (2)));; (* (λx.x)2 → 2 *)
- : value = Vint 2
```

Note: To obtain improved performance one should implement environments by persistent extensible arrays: for instance by the Vec library by Luca de Alfaro.
Subtyping
Outline

4 Simple Types

5 Recursive Types

6 Bibliography
4 Simple Types

5 Recursive Types

6 Bibliography
Simply Typed λ-calculus

Syntax

Types \( T \) ::= \( T \to T \)  
function types  

<table>
<thead>
<tr>
<th>Bool</th>
<th>Int</th>
<th>Real</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>basic types</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Terms \( a, b \) ::= true | false | 1 | 2 | ...  
constants  

<table>
<thead>
<tr>
<th>x</th>
</tr>
</thead>
<tbody>
<tr>
<td>variable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ab</th>
</tr>
</thead>
<tbody>
<tr>
<td>application</td>
</tr>
</tbody>
</table>

| \( \lambda x : T.a \)  
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>abstraction</td>
</tr>
</tbody>
</table>

Reduction

Contexts \( C[] \) ::= [] \( a[] \) \( []a \) \( \lambda x : T.[] \)

\( \text{BETA} \)

\( (\lambda x : T.a)b \rightarrow a[b/x] \)

\( \text{CONTEXT} \)

\( a \rightarrow b \)

\( C[a] \rightarrow C[b] \)
Type system

Typing

\[ \text{VAR} \]
\[ \Gamma \vdash x : \Gamma(x) \]

\[ \rightarrow \text{INTRO} \]
\[ \Gamma, x : S \vdash a : T \]
\[ \Gamma \vdash \lambda x : S. a : S \rightarrow T \]

\[ \rightarrow \text{ELIM} \]
\[ \Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S \]
\[ \Gamma \vdash ab : T \]

(plus the typing rules for constants).
Type system

Typing

\[
\begin{align*}
\text{VAR} & \quad \Gamma \vdash x : \Gamma(x) \\
\rightarrow \text{INTRO} & \quad \Gamma, x : S \vdash a : T \\
& \quad \Gamma \vdash \lambda x : S . a : S \rightarrow T \\
\rightarrow \text{ELIM} & \quad \Gamma \vdash a : S \rightarrow T \\
& \quad \Gamma \vdash b : S \\
& \quad \Gamma \vdash ab : T
\end{align*}
\]

(plus the typing rules for constants).

Theorem (Subject Reduction)

If \( \Gamma \vdash a : T \) and \( a \to^* b \), then \( \Gamma \vdash b : T \).
Type system

Typing

\[ \begin{align*} 
\text{VAR} & \quad \Gamma \vdash x : \Gamma(x) \\
\rightarrow \text{INTRO} & \quad \Gamma, x : S \vdash a : T \\
& \quad \Gamma \vdash \lambda x : S. a : S \rightarrow T \\
\rightarrow \text{ELIM} & \quad \Gamma \vdash a : S \rightarrow T \\
& \quad \Gamma, x : S \vdash a : T \\
& \quad \Gamma \vdash b : S \\
& \quad \Gamma \vdash ab : T \\
\end{align*} \]

(plus the typing rules for constants).

Theorem (Subject Reduction)

If \( \Gamma \vdash a : T \) and \( a \xrightarrow{*} b \), then \( \Gamma \vdash b : T \).

We will essentially focus on the subject reduction property (a.k.a. type preservation), though well-typed programs must also satisfy progress:

Theorem (Progress)

If \( \emptyset \vdash a : T \) and \( a \not\rightarrow \), then \( a \) is a value

where a value is either a constant or a lambda abstraction

\[ v ::= \lambda x : T. a \mid \text{true} \mid \text{false} \mid 1 \mid 2 \mid \ldots \]
A type system is *sound* if every well-typed expression either diverges or reduces to a value of type

Soundness is a corollary of subject reduction and progress
Type checking algorithm

The deduction system is \textit{syntax directed} and satisfies the \textit{subformula property}. As such it describes a deterministic algorithm.
Type checking algorithm

The deduction system is *syntax directed* and satisfies the *subformula property*. As such it describes a deterministic algorithm.

```ml
let rec typecheck gamma = function
  | x -> gamma(x)            (* Var rule *)
  | \x:T.a -> T \rightarrow (typecheck (gamma, x:T) a) (* Intro rule *)
  | a\ b -> let T_1 \rightarrow T_2 = typecheck gamma a in
            (* Elim rule *)
              let T_3 = typecheck gamma b in
            if T_1 == T_3 then T_2 else fail
```

**Exercise.** Write the typecheck function for the following definitions:

- `type stype = Int | Bool | Arrow of stype * stype`
- `type term = Num of int | BVal of bool | Var of string | Lam of string * stype * term | App of term * term`
- `exception Error`

Use `List.assoc` for environments.
Type checking algorithm

The deduction system is *syntax directed* and satisfies the *subformula property*. As such it describes a deterministic algorithm.

```ocaml
let rec typecheck gamma = function
  | x -> gamma(x) (* Var rule *)
  | \x:T.a -> T \rightarrow (typecheck (gamma, x:T) a) (* Intro rule *)
  | a b -> let T_1 \rightarrow T_2 = typecheck gamma a in
         let T_3 = typecheck gamma b in
         if T_1 == T_3 then T_2 else fail
```

**Exercise.** Write the *typecheck* function for the following definitions:

```ocaml
type stype = Int | Bool | Arrow of stype * stype

type term =
  Num of int | BVal of bool | Var of string
  | Lam of string * stype * term | App of term * term

exception Error

Use *List.assoc* for environments.
Subtyping

The rule for application requires the argument of the function to be *exactly of the same type* as the domain of the function:

\[
\rightarrow_\text{ELIM} \\
\Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S \\
\hline \\
\Gamma \vdash ab : T
\]

So, for instance, we **cannot**:

- Apply a function of type `Int → Int` to an argument of type `Odd even` though every odd number is an integer number, too.
- Apply the function `λ x : {ℓ : Int} . (3 + x.ℓ)` to a record of type `{ℓ : Int, ℓ′ : Bool}`.
- In OOP, send a message defined for objects of the class `Persons` to an instance of the subclass `Students`.
Subtyping

The rule for application requires the argument of the function to be *exactly of the same type* as the domain of the function:

\[ \rightarrow \text{ELIM} \]

\[ \Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S \]

\[ \Gamma \vdash ab : T \]

So, for instance, we **cannot**:

- Apply a function of type \( \text{Int} \rightarrow \text{Int} \) to an argument of type \( \text{Odd} \) even though every odd number is an integer number, too.
Subtyping

The rule for application requires the argument of the function to be \textit{exactly of the same type} as the domain of the function:

\[
\Gamma \vdash \mathit{→ELIM} \\
\Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S \\
\Gamma \vdash ab : T
\]

So, for instance, we \textbf{cannot}:

- Apply a function of type \texttt{Int \rightarrow Int} to an argument of type \texttt{Odd} even though every odd number is an integer number, too.
- If we have records, apply the function \(\lambda x: \{\ell : \text{Int}\}.(3 + x.\ell)\) to a record of type \(\{\ell : \text{Int}, \ell' : \text{Bool}\}\)
Subtyping

The rule for application requires the argument of the function to be \textit{exactly of the same type} as the domain of the function:

\[
\begin{align*}
\text{\textit{\text{\rightarrow ELIM}}} \\
\Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S \\
\hline
\Gamma \vdash ab : T
\end{align*}
\]

So, for instance, we \textbf{cannot}:

- Apply a function of type \texttt{Int} → \texttt{Int} to an argument of type \texttt{Odd} even though every odd number is an integer number, too.
- If we have records, apply the function \(\lambda x: \{\ell : \texttt{Int}\}.(3 + x.\ell)\) to a record of type \(\{\ell : \texttt{Int}, \ell' : \texttt{Bool}\}\)
- If we are in OOP, send a message defined for objects of the class \texttt{Persons} to an instance of the subclass \texttt{Students}. 
Subtyping

The rule for application requires the argument of the function to be *exactly of the same type* as the domain of the function:

$$
\rightarrow_{\text{ELIM}}
\quad \Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S \\
\therefore \quad \Gamma \vdash ab : T
$$

So, for instance, we **cannot**:

- Apply a function of type $\text{Int} \rightarrow \text{Int}$ to an argument of type $\text{Odd}$ even though every odd number is an integer number, too.
- If we have records, apply the function $\lambda x:\{\ell : \text{Int}\}.(3 + x.\ell)$ to a record of type $\{\ell : \text{Int}, \ell' : \text{Bool}\}$
- If we are in OOP, send a message defined for objects of the class $\text{Persons}$ to an instance of the subclass $\text{Students}$.

Subtyping polymorphism

We need a kind of polymorphism different from the ML one (parametric polymorphism).
Define a pre-order (i.e., a reflexive and transitive binary relation) $\leq$ on types: $\leq \subset Types \times Types$ (some literature uses the notation $<:$). This subtyping relation has two possible interpretations:

- **Containment:** If $S \leq T$, then every value of type $S$ is also of type $T$. For instance, an odd number is also an integer, a student is also a person. Sometimes called a "is_a" relation.
- **Substitutability:** If $S \leq T$, then every value of type $S$ can be safely used where a value of type $T$ is expected. Where "safely" means, without disrupting type preservation and progress.

We'll see how each interpretation has a formal counterpart.
Subtyping relation

- Define a pre-order (i.e., a reflexive and transitive binary relation) \( \leq \) on types: \( \leq \subseteq \ Types \times \ Types \) (some literature uses the notation \( <: \))
- This *subtyping relation* has two possible interpretations:
Define a pre-order (ie, a reflexive and transitive binary relation) $\leq$ on types: $\leq \subset \text{Types} \times \text{Types}$ (some literature uses the notation $<:$)

This subtyping relation has two possible interpretations:

**Containment:** If $S \leq T$, then every value of type $S$ is also of type $T$. For instance an odd number is also an integer, a student is also a person. Sometimes called a “is_a” relation.
Subtyping relation

- Define a pre-order (i.e., a reflexive and transitive binary relation) \( \leq \) on types: \( \leq \subset \text{Types} \times \text{Types} \) (some literature uses the notation \( <: \))

- This *subtyping relation* has two possible interpretations:

  **Containment:** If \( S \leq T \), then every value of type \( S \) is *also* of type \( T \).
  For instance an odd number is *also* an integer, a student is *also* a person.

  Sometimes called a “is_a” relation.

  **Substitutability:** If \( S \leq T \), then every value of type \( S \) can be *safely* used where a value of type \( T \) is expected.

  Where “safely” means, without disrupting type preservation and progress.
Define a pre-order (i.e., a reflexive and transitive binary relation) \( \leq \) on types: \( \leq \subseteq \text{Types} \times \text{Types} \) (some literature uses the notation \(<:\))

This subtyping relation has two possible interpretations:

**Containment:** If \( S \leq T \), then every value of type \( S \) is also of type \( T \). For instance, an odd number is also an integer, a student is also a person. Sometimes called a “is_a” relation.

**Substitutability:** If \( S \leq T \), then every value of type \( S \) can be safely used where a value of type \( T \) is expected. Where “safely” means, without disrupting type preservation and progress.

We’ll see how each interpretation has a formal counterpart.
We suppose to have a predefined preorder $\mathcal{B} \subseteq \text{Basic} \times \text{Basic}$ for basic types (given by the language designer).

For instance take the reflexive and transitive closure of

\{(Odd, Int), (Even, Int), (Int, Real)\}
We suppose to have a predefined preorder $B \subseteq \text{Basic} \times \text{Basic}$ for basic types (given by the language designer).

For instance take the reflexive and transitive closure of
$\{(\text{Odd}, \text{Int}), (\text{Even}, \text{Int}), (\text{Int}, \text{Real})\}$

To extend it to function types, we resort to the substitutability interpretation. We will try to deduce when we can safely replace a function of some type by a term of a different type.
Subtyping of arrows: intuition

Problem

Determine for which type $S$ we have $S \leq T_1 \to T_2$

Let $g : S$ and $f : T_1 \to T_2$. Let us follow the substitutability interpretation:
Subtyping of arrows: intuition

Problem

Determine for which type $S$ we have $S \leq T_1 \rightarrow T_2$

Let $g : S$ and $f : T_1 \rightarrow T_2$. Let us follow the substitutability interpretation:

1. If $a : T_1$, then we can apply $f$ to $a$. If $S \leq T_1 \rightarrow T_2$, then we can apply $g$ to $a$, as well.

$\Rightarrow g$ is a function, therefore $S = S_1 \rightarrow S_2$
Determine for which type $S$ we have $S \leq T_1 \rightarrow T_2$

Let $g : S$ and $f : T_1 \rightarrow T_2$. Let us follow the **substitutability interpretation**:

1. If $a : T_1$, then we can apply $f$ to $a$. If $S \leq T_1 \rightarrow T_2$, then we can apply $g$ to $a$, as well.
   \[ \Rightarrow g \text{ is a function, therefore } S = S_1 \rightarrow S_2 \]

2. If $a : T_1$, then $f(a)$ is well typed. If $S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2$, then also $g(a)$ is well-typed. $g$ expects arguments of type $S_1$ but $a$ is of type $T_1$.
   \[ \Rightarrow \text{we can safely use } T_1 \text{ where } S_1 \text{ is expected, ie } T_1 \leq S_1 \]
Subtyping of arrows: intuition

Problem

Determine for which type $S$ we have $S \leq T_1 \rightarrow T_2$

Let $g : S$ and $f : T_1 \rightarrow T_2$. Let us follow the substitutability interpretation:

1. If $a : T_1$, then we can apply $f$ to $a$. If $S \leq T_1 \rightarrow T_2$, then we can apply $g$ to $a$, as well.

   $\Rightarrow$ $g$ is a function, therefore $S = S_1 \rightarrow S_2$

2. If $a : T_1$, then $f(a)$ is well-typed. If $S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2$, then also $g(a)$ is well-typed. $g$ expects arguments of type $S_1$ but $a$ is of type $T_1$

   $\Rightarrow$ we can safely use $T_1$ where $S_1$ is expected, ie $T_1 \leq S_1$

3. $f(a) : T_2$, but since $g$ returns results in $S_2$, then $g(a) : S_2$. If I use $g$ where $f$ is expected, then it must be safe to use $S_2$ results where $T_2$ results are expected

   $\Rightarrow$ $S_2 \leq T_2$ must hold.
Subtyping of arrows: intuition

Problem
Determine for which type $S$ we have $S \leq T_1 \to T_2$

Let $g : S$ and $f : T_1 \to T_2$. Let us follow the **substitutability interpretation**:

1. If $a : T_1$, then we can apply $f$ to $a$. If $S \leq T_1 \to T_2$, then we can apply $g$ to $a$, as well.
   \[ \Rightarrow g \text{ is a function, therefore } S = S_1 \to S_2 \]
2. If $a : T_1$, then $f(a)$ is well typed. If $S_1 \to S_2 \leq T_1 \to T_2$, then also $g(a)$ is well-typed. $g$ expects arguments of type $S_1$ but $a$ is of type $T_1$
   \[ \Rightarrow \text{we can safely use } T_1 \text{ where } S_1 \text{ is expected, ie } T_1 \leq S_1 \]
3. $f(a) : T_2$, but since $g$ returns results in $S_2$, then $g(a) : S_2$. If I use $g$ where $f$ is expected, then it must be safe to use $S_2$ results where $T_2$ results are expected
   \[ \Rightarrow S_2 \leq T_2 \text{ must hold.} \]

Solution
$S_1 \to S_2 \leq T_1 \to T_2 \iff T_1 \leq S_1 \text{ and } S_2 \leq T_2$
Covariance and contravariance

\[ S_1 \to S_2 \leq T_1 \to T_2 \iff T_1 \leq S_1 \text{ and } S_2 \leq T_2 \]

Notice the different orientation of containment on domains and co-domains. We say that the type constructor \( \to \) is

- **covariant** on codomains, since it preserves the direction of the relation;
- **contravariant** on domains, since it reverses the direction of the relation.
S_1 \to S_2 \leq T_1 \to T_2 \iff T_1 \leq S_1 \text{ and } S_2 \leq T_2

Notice the different orientation of containment on domains and co-domains. We say that the type constructor \( \to \) is

- **covariant** on codomains, since it preserves the direction of the relation;
- **contravariant** on domains, since it reverses the direction of the relation.

**Containment interpretation:**
The *containment interpretation* yields exactly the same relation as obtained by the *substitutability interpretation*. For instance a function that maps integers to integers ...

\[ \text{Int} \to \text{Int} \leq \text{Int} \to \text{Real} \text{ (covariance of the codomains)} \]

\[ \text{Int} \to \text{Int} \leq \text{Odd} \to \text{Int} \text{ (contravariance of the codomains)} \]
Covariance and contravariance

\[ S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2 \iff T_1 \leq S_1 \text{ and } S_2 \leq T_2 \]

Notice the different orientation of containment on domains and co-domains. We say that the type constructor \( \rightarrow \) is

- **covariant** on codomains, since it preserves the direction of the relation;
- **contravariant** on domains, since it reverses the direction of the relation.

**Containment interpretation:**
The *containment interpretation* yields exactly the same relation as obtained by the *substitutability interpretation*. For instance a function that maps integers to integers ...

- *is also* a function that maps integers to reals: it returns results in \( \text{Int} \) so they will be also in \( \text{Real} \).

\( \text{Int} \rightarrow \text{Int} \leq \text{Int} \rightarrow \text{Real} \) (covariance of the codomains)
Covariance and contravariance

\[ S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2 \iff T_1 \leq S_1 \text{ and } S_2 \leq T_2 \]

Notice the different orientation of containment on domains and co-domains.
We say that the type constructor \( \rightarrow \) is

- **covariant** on codomains, since it preserves the direction of the relation;
- **contravariant** on domains, since it reverses the direction of the relation.

**Containment interpretation:**
The *containment interpretation* yields exactly the same relation as obtained by the *substitutability interpretation*. For instance a function that maps integers to integers ...

- *is also* a function that maps integers to reals: it returns results in \( \text{Int} \) so they will be also in \( \text{Real} \).
  \[ \text{Int} \rightarrow \text{Int} \leq \text{Int} \rightarrow \text{Real} \]  (covariance of the codomains)
- *is also* a function that maps odds to integers: when fed with integers it returns integers, so will do the same when fed with odd numbers.
  \[ \text{Int} \rightarrow \text{Int} \leq \text{Odd} \rightarrow \text{Int} \]  (contravariance of the codomains)
Subtyping deduction system

\[ \begin{align*}
\text{BASIC} \quad & (B_1, B_2) \in \mathcal{B} \quad \Rightarrow \quad B_1 \leq B_2 \\
\text{REFL} \quad & \quad \Rightarrow \quad T \leq T \\
\text{ARROW} \quad & T_1 \leq S_1 \quad S_2 \leq T_2 \quad \Rightarrow \quad S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2 \\
\text{TRANS} \quad & T_1 \leq T_2 \quad T_2 \leq T_3 \quad \Rightarrow \quad T_1 \leq T_3
\end{align*} \]

How do we define an algorithm to check the subtyping relation?

Theorem (Admissibility of Refl and Trans)

1) \( T \leq T \) is provable for all types \( T \)
2) If \( T_1 \leq T_2 \) and \( T_2 \leq T_3 \) are provable, so is \( T_1 \leq T_3 \).

The rules Refl and Trans are admissible.
Subtyping deduction system

<table>
<thead>
<tr>
<th>Rule</th>
<th>Premise</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>B</strong>asic</td>
<td>((B_1, B_2) \in \mathcal{B})</td>
<td>(B_1 \leq B_2)</td>
</tr>
<tr>
<td><strong>R</strong>elf</td>
<td>(T \leq T)</td>
<td>(T \leq T)</td>
</tr>
<tr>
<td><strong>A</strong>rrow</td>
<td>(T_1 \leq S_1) (\quad) (S_2 \leq T_2)</td>
<td>(S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2)</td>
</tr>
<tr>
<td><strong>T</strong>rans</td>
<td>(T_1 \leq T_2) (\quad) (T_2 \leq T_3)</td>
<td>(T_1 \leq T_3)</td>
</tr>
</tbody>
</table>

This system is neither *syntax directed* nor satisfies the *subformula* property.
Subtyping deduction system

\[ (B_1, B_2) \in \mathcal{B} \quad \Rightarrow \quad B_1 \leq B_2 \]

\[ \text{ARROW} \quad \frac{T_1 \leq S_1 \quad S_2 \leq T_2}{S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2} \]

\[ \text{REFL} \quad \frac{T \leq T}{T} \]

\[ \text{TRANS} \quad \frac{T_1 \leq T_2 \quad T_2 \leq T_3}{T_1 \leq T_3} \]

This system is neither *syntax directed* nor satisfies the *subformula* property.

How do we define an algorithm to check the subtyping relation?
Subtyping deduction system

\[
\begin{align*}
\text{BASIC} & \quad (B_1, B_2) \in \mathcal{B} \
& \quad \Rightarrow B_1 \leq B_2 \\
\text{ARROW} & \quad T_1 \leq S_1 \quad S_2 \leq T_2 \\
& \quad \Rightarrow S_1 \to S_2 \leq T_1 \to T_2
\end{align*}
\]

How do we define an algorithm to check the subtyping relation?
These rules describe a deterministic and terminating algorithm (we say that the system is algorithmic).

How do we define an algorithm to check the subtyping relation?
Subtyping deduction system

\[
\begin{align*}
\text{BASIC} & \quad (B_1, B_2) \in \mathcal{B} \\
& \quad \Rightarrow B_1 \leq B_2 \\
\text{ARROW} & \quad T_1 \leq S_1 \quad S_2 \leq T_2 \\
& \quad S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2
\end{align*}
\]

These rules describe a deterministic and terminating algorithm (we say that the system is algorithmic).

How do we define an algorithm to check the subtyping relation?

Theorem (Admissibility of Refl and Trans)

*In the system composed just by the rules Arrow and Basic:*

1) \( T \leq T \) is provable for all types \( T \)

2) If \( T_1 \leq T_2 \) and \( T_2 \leq T_3 \) are provable, so is \( T_1 \leq T_3 \).

The rules Refl and Trans are *admissible*
We defined the subtyping relation and we know how to decide it. How do we use it for typing our programs?
We defined the subtyping relation and we know how to decide it. How do we use it for typing our programs?

$$\text{VAR} \quad \frac{\text{Γ} \vdash x : \Gamma(x)}{\text{Γ} \vdash a : T} \quad \text{→INTRO}$$

$$\frac{\text{Γ} \vdash \lambda x : S. a : S \rightarrow T}{\text{Γ} \vdash ab : T} \quad \text{→ELIM}$$

This corresponds to the containment relation: if $S \leq T$ and $a$ is of type $S$ then $a$ is also of type $T$.

Subject reduction: If $\Gamma \vdash a : T$ and $a \rightarrow^* b$, then $\Gamma \vdash b : T$.

Progress property: If $\emptyset \vdash a : T$ and $a \not\rightarrow$, then $a$ is a value.
We defined the subtyping relation and we know how to decide it. How do we use it for typing our programs?

\[
\begin{align*}
\text{VAR} & \quad \text{INTRO} & \text{ELIM} \\
\Gamma \vdash x : \Gamma(x) & \quad \Gamma, x : S \vdash a : T & \quad \Gamma \vdash a : S \rightarrow T \\
& \quad \Gamma \vdash \lambda x : S. a : S \rightarrow T & \quad \Gamma \vdash b : S \\
& \quad \Gamma \vdash a : S \leq T & \quad \Gamma \vdash ab : T \\
\end{align*}
\]
We defined the subtyping relation and we know how to decide it. How do we use it for typing our programs?

This corresponds to the containment relation:

if $S \leq T$ and $a$ is of type $S$ then $a$ is also of type $T$
Type system

We defined the subtyping relation and we know how to decide it. How do we use it for typing our programs?

\[
\begin{align*}
\textsc{var} & \quad \Gamma \vdash x : \Gamma(x) \\
\textsc{intro} & \quad \Gamma, x : S \vdash a : T \\
& \quad \frac{}{\Gamma \vdash \lambda x : S. a : S \to T}
\end{align*}
\]

\[
\begin{align*}
\textsc{elim} & \quad \Gamma \vdash a : S \to T \quad \Gamma \vdash b : S \\
& \quad \frac{}{\Gamma \vdash ab : T}
\end{align*}
\]

\[
\begin{align*}
\textsc{subsumption} & \quad \Gamma \vdash a : S \\
& \quad \frac{S \leq T}{\Gamma \vdash a : T}
\end{align*}
\]

This corresponds to the *containment relation*:

If \( S \leq T \) and \( a \) is of type \( S \) then \( a \) is also of type \( T \)

**Subject reduction:** If \( \Gamma \vdash a : T \) and \( a \xrightarrow{*} b \), then \( \Gamma \vdash b : T \).

**Progress property:** If \( \emptyset \vdash a : T \) and \( a \xrightarrow{\not\cdot} \), then \( a \) is a value.
Typing algorithm

\[ \text{VAR} \]
\[ \Gamma \vdash x : \Gamma(x) \]

\[ \text{→INTRO} \]
\[ \frac{\Gamma, x : S \vdash a : T}{\Gamma \vdash \lambda x : S. a : S \rightarrow T} \]

\[ \text{→ELIM} \]
\[ \frac{\Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S}{\Gamma \vdash ab : T} \]

\[ \text{SUBSUMPTION} \]
\[ \frac{\Gamma \vdash a : S \quad S \leq T}{\Gamma \vdash a : T} \]

Subsumption makes the type system non-algorithmic: it is not syntax directed; subsumption can be applied whatever the term. It does not satisfy the subformula property: even if we know that we have to apply subsumption which shall we choose? How do we define the typechecking algorithm?
Typing algorithm

\(\text{VAR} \quad \Gamma \vdash x : \Gamma(x) \quad \rightarrow\text{INTRO} \quad \Gamma, x : S \vdash a : T \quad \frac{}{\Gamma \vdash \lambda x:S.a : S \rightarrow T} \)

\(\rightarrow\text{ELIM} \quad \Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S \quad \frac{}{\Gamma \vdash ab : T} \quad \text{SUBSUMPTION} \quad \Gamma \vdash a : S \quad S \leq T \quad \frac{}{\Gamma \vdash a : T} \)

Subsumption makes the type system non-algorithmic:

- it is not \textit{syntax directed}: subsumption can be applied whatever the term.
- it does not satisfy the \textit{subformula property}: even if we know that we have to apply subsumption which \(T\) shall we choose?
Typing algorithm

\[ \text{VAR} \]
\[ \Gamma \vdash x : \Gamma(x) \]

\[ \text{⇒ INTRO} \]
\[ \Gamma, x : S \vdash a : T \]
\[ \Gamma \vdash \lambda x:S.a : S \rightarrow T \]

\[ \text{⇒ ELIM} \]
\[ \Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S \]
\[ \Gamma \vdash ab : T \]

\[ \text{SUBSUMPTION} \]
\[ \Gamma \vdash a : S \quad S \leq T \]
\[ \Gamma \vdash a : T \]

Subsumption makes the type system non-algorithmic:

- it is not \textit{syntax directed}: subsumption can be applied whatever the term.
- it does not satisfy the \textit{subformula property}: even if we know that we have to apply subsumption which \( T \) shall we choose?

How do we define the typechecking algorithm?
Subsumption makes the type system non-algorithmic:

- it is not *syntax directed*: subsumption can be applied whatever the term.
- it does not satisfy the *subformula property*: even if we know that we have to apply subsumption which $T$ shall we choose?

How do we define the typechecking algorithm?
Typing algorithm

\[ \text{VAR} \]
\[ \Gamma \vdash_{\mathcal{A}} x : \Gamma(x) \]

\[ \text{→INTRO} \]
\[ \Gamma, x : S \vdash_{\mathcal{A}} a : T \]
\[ \frac{}{\Gamma \vdash_{\mathcal{A}} \lambda x : S. a : S \rightarrow T} \]

\[ \text{→ELIM}_{\leq} \]
\[ \Gamma \vdash_{\mathcal{A}} a : S \rightarrow T \quad \Gamma \vdash_{\mathcal{A}} b : U \quad U \leq S \]
\[ \frac{}{\Gamma \vdash_{\mathcal{A}} a b : T} \]

1. The system is algorithmic: it describes a typing algorithm (exercise: program typecheck and subtype by using the previous structures).

2. The system conforms the substitutability interpretation: we use an expression of a subtype \( U \) where a supertype \( S \) is expected (note “use” = elimination rule).
Typing algorithm

1. The system is algorithmic: it describes a typing algorithm (exercise: program typecheck and subtype by using the previous structures).
2. The system conforms the substitutability interpretation: we use an expression of a subtype $U$ where a supertype $S$ is expected (note “use” = elimination rule).

How do we relate the two systems?
Typing algorithm

\[ \text{The system is algorithmic: it describes a typing algorithm (exercise: program typecheck and subtype by using the previous structures).} \]

\[ \text{The system conforms the substitutability interpretation: we use an expression of a subtype } U \text{ where a supertype } S \text{ is expected (note “use” = elimination rule).} \]

How do we relate the two systems?

For subtyping, admissibility ensured that the system and the algorithm prove the same judgements. Here it is no longer true. For instance:

\[ \emptyset \vdash \lambda x:\text{Int}.x : \text{Odd} \rightarrow \text{Real} \]  

\[ \emptyset \not\vdash \lambda x:\text{Int}.x : \text{Odd} \rightarrow \text{Real}. \]
Typing algorithm

\[\text{VAR} \quad \Gamma \vdash \text{A} x : \Gamma(x) \quad \rightarrow \text{INTRO} \quad \frac{\Gamma, x : S \vdash \text{A} a : T}{\Gamma \vdash \text{A} \lambda x : S. a : S \rightarrow T} \quad \rightarrow \text{ELIM} \leq \quad \frac{\Gamma \vdash \text{A} a : S \rightarrow T \quad \Gamma \vdash \text{A} b : U \quad U \leq S}{\Gamma \vdash \text{A} ab : T}\]

The system is algorithmic: it describes a typing algorithm (exercise: program typecheck and subtype by using the previous structures)

The system conforms the substitutability interpretation: we use an expression of a subtype \( U \) where a supertype \( S \) is expected (note “use” = elimination rule).

How do we relate the two systems?

For subtyping, admissibility ensured that the system and the algorithm prove the same judgements. Here it is no longer true. For instance:

\[\emptyset \vdash \lambda x : \text{Int}. x : \text{Odd} \rightarrow \text{Real} \quad \text{but} \quad \emptyset \not\vdash \text{A} \lambda x : \text{Int}. x : \text{Odd} \rightarrow \text{Real}.\]

This is expected: Algorithm = one type returned for each typable term.
Soundness and completeness of the typing algorithm

\[
a \text{is typable by } \vdash \iff a \text{ is typable by } \vdash A
\]

\[
\iff = \text{soundness}
\implies = \text{completeness}
\]
Soundness and completeness of the typing algorithm

\[ a \text{ is typable by } \vdash \iff a \text{ is typable by } \vdash A \]

\[ \iff = \text{ soundness} \]
\[ \implies = \text{ completeness} \]

**Theorem (Soundness)**

*If* \( \Gamma \vdash_A a : T \), *then* \( \Gamma \vdash a : T \)

**Theorem (Completeness)**

*If* \( \Gamma \vdash a : T \), *then* \( \Gamma \vdash_A a : S \) with \( S \leq T \)
Corollary (Minimum type)

\[ \text{If } \Gamma \vdash \_ \ a : T \text{ then } T = \min \{ S \mid \Gamma \vdash a : S \} \]

**Proof.** Let \( S = \{ S \mid \Gamma \vdash a : S \} \). Soundness ensures that \( S \) is not empty. Completeness states that \( T \) is a lower bound of \( S \). Minimality follows by using soundness once more.
Corollary (Minimum type)

If $\Gamma \vdash a : T$ then $T = \min \{ S \mid \Gamma \vdash a : S \}$

Proof. Let $S = \{ S \mid \Gamma \vdash a : S \}$. Soundness ensures that $S$ is not empty. Completeness states that $T$ is a lower bound of $S$. Minimality follows by using soundness once more.

The corollary above explains that the typing algorithm works with the minimum types of the terms. It keeps track of the best type information available.
**Corollary (Minimum type)**

\[ \text{If } \Gamma \vdash a : T \text{ then } T = \min\{S \mid \Gamma \vdash a : S\} \]

**Proof.** Let \( S = \{S \mid \Gamma \vdash a : S\} \). Soundness ensures that \( S \) is not empty. Completeness states that \( T \) is a lower bound of \( S \). Minimality follows by using soundness once more.

The corollary above explains that the typing algorithm works with the minimum types of the terms. It keeps track of the best type information available.

**Theorem (Algorithmic subject reduction)**

\[ \text{If } \Gamma \vdash a : T \text{ and } a \rightarrow^* b, \text{ then } \Gamma \vdash b : S \text{ with } S \leq T. \]

The theorem above explains that the computation reduces the minimum type of a program. As such it increases the type information about it.
Summary for simply-typed $\lambda$-calculs $+$ $\leq$

- The *containment* interpretation of the subtyping relation corresponds to the "logical" view of the type system embodied by subsumption.
- The *substitutability* interpretation of the subtyping relation corresponds to the "algorithmic" view of the type system.
Summary for simply-typed $\lambda$-calculus + $\leq$

- The *containment* interpretation of the subtyping relation corresponds to the “logical” view of the type system embodied by subsumption.
- The *substitutability* interpretation of the subtyping relation corresponds to the “algorithmic” view of the type system.
- To *define* the type system one usually starts from the “logical” system, which is simpler since subtyping is concentrated in the subsumption rule.
- To *implement* the type system one passes to the substitutability view. Subsumption is eliminated and the check of the subtyping relation is distributed in the places where values are used/consumed. This in general corresponds to embed subtype checking into elimination rules.
The *containment* interpretation of the subtyping relation corresponds to the “logical” view of the type system embodied by subsumption.

The *substitutability* interpretation of the subtyping relation corresponds to the “algorithmic” view of the type system.

To *define* the type system one usually starts from the “logical” system, which is simpler since subtyping is concentrated in the subsumption rule.

To *implement* the type system one passes to the substitutability view. Subsumption is eliminated and the check of the subtyping relation is distributed in the places where values are used/consumed. This in general corresponds to embed subtype checking into elimination rules.

The obtained algorithm works on the *minimum types* of the logical system.

Computation reduces the (algorithmic) type thus increasing type information (the result of a computation represents the best possible type information: it is the *singleton type* containing the result).

The last point makes *dynamic dispatch* (aka, dynamic binding) meaningful.
Products I

Syntax

Types \( T \) ::= ... \( T \times T \)  
product types

Terms \( a, b \) ::= ...

| \( (a, a) \)  
| \( \pi_i(a) \quad (i=1,2) \)  
| pair  
| projection

Reduction

\[ \pi_i((a_1, a_2)) \rightarrow a_i \quad (i=1,2) \]

Typing

\( \times \text{INTRO} \)

\[ \Gamma \vdash a_1 : T_1 \quad \Gamma \vdash a_2 : T_2 \]

\[ \Gamma \vdash (a_1, a_2) : T_1 \times T_2 \]

\( \times \text{ELIM}_i \)

\[ \Gamma \vdash a : T_1 \times T_2 \]

\[ \Gamma \vdash \pi_i(a) : T_i \quad (i=1,2) \]
Subtyping

\[ \text{PROD} \]
\[ S_1 \leq T_1 \quad S_2 \leq T_2 \]
\[ S_1 \times S_2 \leq T_1 \times T_2 \]

**Exercise:** Check whether the above rule is compatible with the containment and/or the substitutability interpretation of the subtyping relation.

The subtyping rule above is also algorithmic. Similarly, for the typing rules there is no need to embed subtyping in the elimination rules since \( \pi_i \) is an operator that works on all products, not a particular one (cf. with the application of a function, which requires a particular domain).

Of course subject reduction and progress still hold.

**Exercise:** Define values and reduction contexts for this extension.
Records

Up to now subtyping rules « lift » the subtyping relation $\mathcal{B}$ on basic types to constructed types. But if $\mathcal{B}$ is the identity relation, so is the whole subtyping relation. Record subtyping is non-trivial even when $\mathcal{B}$ is the identity relation.

Syntax

$$
\begin{align*}
\text{Types} & \quad T ::= \ldots \mid \{ \ell : T, \ldots, \ell : T \} \quad \text{record types} \\
\text{Terms} & \quad a, b ::= \ldots \\
& \quad \mid \{ \ell = a, \ldots, \ell = a \} \quad \text{record} \\
& \quad \mid a.\ell \quad \text{field selection}
\end{align*}
$$

Reduction

$$
\{\ldots, \ell = a, \ldots\}.\ell \rightarrow a
$$

Typing

$$
\begin{align*}
\text{INTRO} & \quad \Gamma \vdash a_1 : T_1 \ldots \Gamma \vdash a_n : T_n \\
& \quad \Gamma \vdash \{\ell_1 = a_1, \ldots, \ell_n = a_n\} : \{\ell_1 : T_1, \ldots, \ell_n : T_n\}
\end{align*}
$$

$$
\begin{align*}
\text{ELIM} & \quad \Gamma \vdash a : \{\ldots, \ell : T, \ldots\} \\
& \quad \Gamma \vdash a.\ell : T
\end{align*}
$$
To define subtyping we resort once more on the substitutability relation. A record is “used” by selecting one of its labels.
Record Subtyping

To define subtyping we resort once more on the substitutability relation. A record is “used” by selecting one of its labels.

We can replace some record by a record of different type if in the latter we can select the same fields as in the former and their contents can substitute the respective contents in the former.

Subtyping

\[
\text{RECORD} \quad S_1 \leq T_1 \ldots S_n \leq T_n \quad \{l_1:S_1,\ldots,l_n:S_n,\ldots,l_{n+k}:S_{n+k}\} \leq \{l_1:T_1,\ldots,l_n:T_n\}
\]

Exercise. Which are the algorithmic typing rules?
Outline

4 Simple Types

5 Recursive Types

6 Bibliography
Iso-recursive and Equi-recursive types

Lists are a classic example of recursive types:

\[ X \approx (\text{Int} \times X) \lor \text{Nil} \]

also written as \( \mu X.((\text{Int} \times X) \lor \text{Nil}) \)

Two different approaches according to whether \( \approx \) is interpreted as an isomorphism or an equality:

**Iso-recursive types:** \( \mu X.((\text{Int} \times X) \lor \text{Nil}) \) is considered *isomorphic* to its one-step unfolding \((\text{Int} \times \mu X.((\text{Int} \times X) \lor \text{Nil})) \lor \text{Nil})\). Terms include a pair of built-in coercion functions for each recursive type \( \mu X. T \):

\[
\begin{align*}
\text{unfold} &: \mu X. T \rightarrow T[\mu X. T/X] \\
\text{fold} &: T[\mu X. T/X] \rightarrow \mu X. T
\end{align*}
\]

**Equi-recursive types:** \( \mu X.((\text{Int} \times X) \lor \text{Nil}) \) is considered *equal* to its one-step unfolding \((\text{Int} \times \mu X.((\text{Int} \times X) \lor \text{Nil})) \lor \text{Nil})\). The two types are completely interchangeable. No support needed from terms.
Iso-recursive and Equi-recursive types

Lists are a classic example of recursive types:

\[ X \approx (\text{Int} \times X) \lor \text{Nil} \]

also written as \( \mu X.((\text{Int} \times X) \lor \text{Nil}) \).

Two different approaches according to whether \( \approx \) is interpreted as an isomorphism or an equality:

**Iso-recursive types:** \( \mu X.((\text{Int} \times X) \lor \text{Nil}) \) is considered *isomorphic* to its one-step unfolding \( (\text{Int} \times \mu X.((\text{Int} \times X) \lor \text{Nil})) \lor \text{Nil} \). Terms include a pair of built-in coercion functions for each recursive type \( \mu X. T \):

\[
\text{unfold} : \mu X. T \rightarrow T[\mu X. T/X] \quad \text{fold} : T[\mu X. T/X] \rightarrow \mu X. T
\]

**Equi-recursive types:** \( \mu X.((\text{Int} \times X) \lor \text{Nil}) \) is considered *equal* to its one-step unfolding \( (\text{Int} \times \mu X.((\text{Int} \times X) \lor \text{Nil})) \lor \text{Nil} \). The two types are completely interchangeable. No support needed from terms.

Subtyping for recursive types generalizes the equi-recursive approach. The \( \approx \) relation corresponds to subtyping in both directions:

\[
\mu X. T \leq T[\mu X. T/X] \quad T[\mu X. T/X] \leq \mu X. T
\]
Recursive types are weird

- To add (equi-)recursive types you do not need to add any new term.

\[
\mu X. (\text{Int} \times X) \lor \text{Nil}
\]

interpret the type above as the finite lists of integers.

Then \(\mu X. (\text{Int} \times X)\) is the empty type.

Actually if you have recursive terms and allow infinite values you can easily jeopardize decidability of the subtyping relation (which resorts to checking type emptiness).

This contrasts with their intuition which looks simple: we always informally applied a rule such as:

\[
A, X \leq Y \vdash S \leq T
\]

\[
A \vdash \mu X. S \leq \mu Y. T
\]
Recursive types are weird

- To add (equi-)recursive types you do not need to add any new term.
- You don’t even need to have recursion on terms:
  \[ \mu X.((\text{Int} \times X) \lor \text{Nil}) \]
  interpret the type above as the *finite* lists of integers.

Then \( \mu X.(\text{Int} \times X) \) is the empty type.
Recursive types are weird

- To add (equi-)recursive types you do not need to add any new term

- You don’t even need to have recursion on terms:
  \[ \mu X.((\text{Int} \times X) \lor \text{Nil}) \]

  interpret the type above as the *finite* lists of integers.

  Then \( \mu X.(\text{Int} \times X) \) is the empty type.

- Actually if you have recursive terms and allow infinite values you can easily jeopardize decidability of the subtyping relation (which resorts to checking type emptiness)

- This contrasts with their intuition which looks simple: we always informally applied a rule such as:

  \[
  A, X \leq Y \vdash S \leq T \\
  \overline{A \vdash \mu X.S \leq \mu Y.T}
  \]
Subtyping recursive types

Syntax

\[ \text{Types} \quad \Gamma \quad ::= \quad \text{Any} \quad \text{top type} \]
\[ \quad | \quad \Gamma \rightarrow \Gamma \quad \text{function types} \]
\[ \quad | \quad \Gamma \times \Gamma \quad \text{product types} \]
\[ \quad | \quad X \quad \text{type variables} \]
\[ \quad | \quad \mu X . \Gamma \quad \text{recursive types} \]

where \( \Gamma \) is \textit{contractive}, that is (two equivalent definitions):

1. \( \Gamma \) is contractive iff for every subexpression \( \mu X . \mu X_1 . . . \mu X_n . S \) it holds \( S \neq X \).
2. \( \Gamma \) is contractive iff every type variable \( X \) occurring in it is separated from its binder by a \( \rightarrow \) or a \( \times \).
Subtyping recursive types

The subtyping relation is defined \textit{COINDUCTIVELY} by the rules:

- **Top**
  
  \[
  \text{T \leq \text{Any}}
  \]

- **Product**
  
  \[
  S_1 \leq T_1 \quad S_2 \leq T_2 \\
  S_1 \times S_2 \leq T_1 \times T_2
  \]

- **Arrow**
  
  \[
  T_1 \leq S_1 \quad S_2 \leq T_2 \\
  S_1 \to S_2 \leq T_1 \to T_2
  \]

- **Unfold Left**
  
  \[
  S[\mu X. S/X] \leq T \\
  \mu X. S \leq T
  \]

- **Unfold Right**
  
  \[
  S \leq T[\mu X. T/X] \\
  S \leq \mu X. T
  \]
Subtyping recursive types

The subtyping relation is defined \textit{COINDUCTIVELY} by the rules

\begin{align*}
\text{TOP} & \quad T \leq \text{Any} \\
\text{PROD} & \quad S_1 \leq T_1, S_2 \leq T_2 \quad \Rightarrow \quad S_1 \times S_2 \leq T_1 \times T_2 \\
\text{ARROW} & \quad T_1 \leq S_1, S_2 \leq T_2 \quad \Rightarrow \quad S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2 \\
\text{UNFOLD LEFT} & \quad S[\mu X. S/X] \leq T \quad \Rightarrow \quad \mu X. S \leq T \\
\text{UNFOLD RIGHT} & \quad S \leq T[\mu X. T/X] \quad \Rightarrow \quad S \leq \mu X. T
\end{align*}

Coinductive definition

1. Why coinduction?
2. Why no reflexivity/transitivity rules?
3. Why no rule to compare two $\mu$-types?
Subtyping recursive types

The subtyping relation is defined **COINDUCTIVELY** by the rules

\[
\begin{align*}
\text{TOP} & \quad T \leq \text{Any} \\
\text{PROD} & \quad S_1 \leq T_1 \quad S_2 \leq T_2 \quad \Rightarrow \quad S_1 \times S_2 \leq T_1 \times T_2 \\
\text{ARROW} & \quad T_1 \leq S_1 \quad S_2 \leq T_2 \quad \Rightarrow \quad S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2 \\
\text{UNFOLD LEFT} & \quad S[\mu X. S/X] \leq T \quad \Rightarrow \quad \mu X. S \leq T \\
\text{UNFOLD RIGHT} & \quad S \leq T[\mu X. T/X] \quad \Rightarrow \quad S \leq \mu X. T
\end{align*}
\]

Coinductive definition

1. Why coinduction?
2. Why no reflexivity/transitivity rules?
3. Why no rule to compare two \(\mu\)-types?

Short answers (more detailed answers to come):

1. Because we compare infinite expansions
2. Because it would be unsound
3. Useless since obtained by coinduction and unfold
Example of coinductive derivation

\[ \text{Even} \leq \text{Int} \quad \mu X.\text{Int} \rightarrow X \leq \mu Y.\text{Even} \rightarrow Y \]

\[ \text{Int} \rightarrow (\mu X.\text{Int} \rightarrow X) \leq \text{Even} \rightarrow (\mu Y.\text{Even} \rightarrow Y) \]

\[ \text{Int} \rightarrow (\mu X.\text{Int} \rightarrow X) \leq \mu Y.\text{Even} \rightarrow Y \]

\[ \mu X.\text{Int} \rightarrow X \leq \mu Y.\text{Even} \rightarrow Y \]
Example of coinductive derivation

\[ \text{even} \leq \text{int} \quad \mu X. \text{int} \rightarrow X \leq \mu Y. \text{even} \rightarrow Y \]

\[ \text{int} \rightarrow (\mu X. \text{int} \rightarrow X) \leq \text{even} \rightarrow (\mu Y. \text{even} \rightarrow Y) \]

\[ \text{int} \rightarrow (\mu X. \text{int} \rightarrow X) \leq \mu Y. \text{even} \rightarrow Y \]

\[ \mu X. \text{int} \rightarrow X \leq \mu Y. \text{even} \rightarrow Y \]

Notice the use of coinduction
Amadio and Cardelli’s subtyping algorithm

Let $A \subset \text{Types} \times \text{Types}$

\[
A \vdash S \leq T \quad (S, T) \in A
\]

\[
A \vdash S \leq \text{Any} \quad (S, \text{Any}) \notin A
\]

\[
A' \vdash S_1 \leq T_1 \quad A' \vdash S_2 \leq T_2 \\
A \vdash S_1 \times S_2 \leq T_1 \times T_2 \\
A' = A \cup (S_1 \times S_2, T_1 \times T_2); A \neq A'
\]

\[
A' \vdash T_1 \leq S_1 \quad A' \vdash S_2 \leq T_2 \\
A \vdash S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2 \\
A' = A \cup (S_1 \rightarrow S_2, T_1 \rightarrow T_2); A \neq A'
\]

\[
A' \vdash S[\mu X.S/X] \leq T \\
A \vdash \mu X.S \leq T \\
A' = A \cup (\mu X.S, T); A \neq A'; T \neq \text{Any}
\]

\[
A' \vdash S \leq T[\mu X.T/X] \\
A \vdash S \leq \mu X.T \\
A' = A \cup (S, \mu X.T); A \neq A'; S \neq \mu Y.U
\]
Amadio and Cardelli’s subtyping algorithm

Determinization of the rules

\[ A \vdash S \leq T \quad (S, T) \in A \]

\[ A \vdash S \leq \text{Any} \quad (S, \text{Any}) \not\in A \]

\[ A' \vdash S_1 \leq T_1 \quad A' \vdash S_2 \leq T_2 \]
\[ A \vdash S_1 \times S_2 \leq T_1 \times T_2 \]

\[ A' = A \cup (S_1 \times S_2, T_1 \times T_2); A \neq A' \]

\[ A' \vdash T_1 \leq S_1 \quad A' \vdash S_2 \leq T_2 \]
\[ A \vdash S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2 \]

\[ A' = A \cup (S_1 \rightarrow S_2, T_1 \rightarrow T_2); A \neq A' \]

\[ A' \vdash S[\mu X.S/X] \leq T \]
\[ A \vdash \mu X.S \leq T \]

\[ A' = A \cup (\mu X.S, T); A \neq A'; T \neq \text{Any} \]

\[ A' \vdash S \leq T[\mu X.T/X] \]
\[ A \vdash S \leq \mu X.T \]

\[ A' = A \cup (S, \mu X.T); A \neq A'; S \neq \mu Y.U \]
Amadio and Cardelli’s subtyping algorithm

Record type to implement coinduction

\[
\frac{A \vdash S \leq T}{(S, T) \in A}
\]

\[
\frac{A \vdash S \leq \text{Any}}{(S, \text{Any}) \not\in A}
\]

\[
\frac{A' \vdash S_1 \leq T_1 \quad A' \vdash S_2 \leq T_2}{A \vdash S_1 \times S_2 \leq T_1 \times T_2}
\]

\[
A' = A \cup (S_1 \times S_2, T_1 \times T_2); A \neq A'
\]

\[
\frac{A' \vdash T_1 \leq S_1 \quad A' \vdash S_2 \leq T_2}{A \vdash S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2}
\]

\[
A' = A \cup (S_1 \rightarrow S_2, T_1 \rightarrow T_2); A \neq A'
\]

\[
\frac{A' \vdash S \mu X. S / X \leq T}{A \vdash S \mu X. S \leq T}
\]

\[
A' = A \cup (\mu X. S, T); A \neq A'; T \neq \text{Any}
\]

\[
A' \vdash S \leq T \mu X. T / X
\]

\[
A' = A \cup (S, \mu X. T); A \neq A'; S \neq \mu Y. U
\]
Amadio and Cardelli’s subtyping algorithm

Determinization of the rules

\[
\frac{A \vdash S \leq T}{A \vdash (S, T) \in A}
\]
\[
\frac{A \vdash S \leq \text{Any}}{(S, \text{Any}) \notin A}
\]
\[
\frac{A' \vdash S_1 \leq T_1 \quad A' \vdash S_2 \leq T_2}{A \vdash S_1 \times S_2 \leq T_1 \times T_2}
\]
\[
A' = A \cup (S_1 \times S_2, T_1 \times T_2); A \neq A'
\]
\[
\frac{A' \vdash T_1 \leq S_1 \quad A' \vdash S_2 \leq T_2}{A \vdash S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2}
\]
\[
A' = A \cup (S_1 \rightarrow S_2, T_1 \rightarrow T_2); A \neq A'
\]
\[
\frac{A' \vdash S[\mu X.S/X] \leq T}{A \vdash \mu X.S \leq T}
\]
\[
A' = A \cup (\mu X.S, T); A \neq A'; T \neq \text{Any}
\]
\[
\frac{A' \vdash S \leq T[\mu X.T/X]}{A \vdash S \leq \mu X.T}
\]
\[
A' = A \cup (S, \mu X.T); A \neq A'; S \neq \mu Y.U
\]
Amadio and Cardelli’s subtyping algorithm

Record type to implement coinduction

\[
\begin{align*}
A \vdash S \leq T & \quad (S, T) \in A \\
A \vdash S \leq \text{Any} & \quad (S, \text{Any}) \not\in A
\end{align*}
\]

\[
\begin{align*}
A' \vdash S_1 \leq T_1 & \quad A' \vdash S_2 \leq T_2 \\
A \vdash S_1 \times S_2 \leq T_1 \times T_2 & \quad A' = A \cup (S_1 \times S_2, T_1 \times T_2); A \neq A'
\end{align*}
\]

\[
\begin{align*}
A' \vdash T_1 \leq S_1 & \quad A' \vdash S_2 \leq T_2 \\
A \vdash S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2 & \quad A' = A \cup (S_1 \rightarrow S_2, T_1 \rightarrow T_2); A \neq A'
\end{align*}
\]

\[
\begin{align*}
A' \vdash S[\mu X.S/X] \leq T & \quad A' = A \cup (\mu X.S, T); A \neq A'; T \neq \text{Any}
\end{align*}
\]

\[
\begin{align*}
A' \vdash S \leq T[\mu X.T/X] & \quad A' = A \cup (S, \mu X.T); A \neq A'; S \neq \mu Y.U
\end{align*}
\]
The rest is similar

\[
\begin{align*}
A \vdash S \leq T & \quad (S, T) \in A \\
A \vdash S \leq \text{Any} & \quad (S, \text{Any}) \notin A \\
A' \vdash S_1 \leq T_1 \quad A' \vdash S_2 \leq T_2 & \quad A' = A \cup (S_1 \times S_2, T_1 \times T_2); A \neq A' \\
A' \vdash T_1 \leq S_1 \quad A' \vdash S_2 \leq T_2 & \quad A' = A \cup (S_1 \to S_2, T_1 \to T_2); A \neq A' \\
A' \vdash S[\mu X. S/X] \leq T & \quad A' = A \cup (\mu X. S, T); A \neq A'; T \neq \text{Any} \\
A' \vdash S \leq T[\mu X. T/X] & \quad A' = A \cup (S, \mu X. T); A \neq A'; S \neq \mu Y. U
\end{align*}
\]
Amadio and Cardelli’s subtyping algorithm

Let $A \subseteq \text{Types} \times \text{Types}$

\[ A \vdash (S, T) \in A \]

\[ A \vdash (S, \text{Any}) \notin A \]

\[ A' \vdash S_1 \leq T_1 \quad A' \vdash S_2 \leq T_2 \]

\[ A \vdash S_1 \times S_2 \leq T_1 \times T_2 \]

\[ A' = A \cup (S_1 \times S_2, T_1 \times T_2); A \neq A' \]

\[ A' \vdash T_1 \leq S_1 \quad A' \vdash S_2 \leq T_2 \]

\[ A \vdash S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2 \]

\[ A' = A \cup (S_1 \rightarrow S_2, T_1 \rightarrow T_2); A \neq A' \]

\[ A' \vdash S[\mu X.S/X] \leq T \]

\[ A \vdash \mu X.S \leq T \]

\[ A' = A \cup (\mu X.S, T); A \neq A'; T \neq \text{Any} \]

\[ A' \vdash S \leq T[\mu X.T/X] \]

\[ A \vdash S \leq \mu X.T \]

\[ A' = A \cup (S, \mu X.T); A \neq A'; S \neq \mu Y.U \]
Theorem (Soundness and Completeness)

Let $S$ and $T$ be closed types. $S \leq T$ belongs the relation coinductively defined by the rules on slide 55 if and only if $\emptyset \vdash S \leq T$ is provable.

Notice that the algorithm above is exponential. We will show how to define an $O(n^2)$ algorithm to decide $S \leq T$, where $n$ is the total number of different subexpressions of $S \leq T$. 
Properties

Theorem (Soundness and Completeness)

Let $S$ and $T$ be closed types. $S \leq T$ belongs the relation coinductively defined by the rules on slide 55 if and only if $\emptyset \vdash S \leq T$ is provable.

Theorem (Soundness and Completeness)

Let $S$ and $T$ be closed types. $S \leq T$ belongs the relation coinductively defined by the rules on slide 55 if and only if $\emptyset \vdash S \leq T$ is provable.


Notice that the algorithm above is exponential. We will show how to define an $O(n^2)$ algorithm to decide $S \leq T$, where $n$ is the total number of different subexpressions of $S \leq T$. 
**Intuition**

Given a deduction system, it characterizes two possible distinct sets (of provable judgements) according to whether an inductive or a coinductive approach is used.

Let $F$ be a deduction system on a universe $U$ (i.e. a monotone function from $P(U)$ to $P(U)$). A set $X \in P(U)$ is:

- $F$-closed if it contains all the elements that can be deduced by $F$ with hypothesis in $X$.
- $F$-consistent if every element of $X$ can be deduced by $F$ from other elements in $X$. 

**Induction and coinduction**

A deduction system inductively defines the least $F$-closed set and coinductively defines the greatest $F$-consistent set.
**Induction and coinduction**

**Intuition**
Given a deduction system, it characterizes two possible distinct sets (of provable judgements) according to whether an inductive or a coinductive approach is used.

Let $\mathcal{F}$ be a deduction system on a universe $\mathcal{U}$ (i.e. a monotone function from $\mathcal{P}(\mathcal{U})$ to $\mathcal{P}(\mathcal{U})$). A set $X \in \mathcal{P}(\mathcal{U})$ is:

- **$\mathcal{F}$-closed** if it contains all the elements that can be deduced by $\mathcal{F}$ with hypothesis in $X$.
- **$\mathcal{F}$-consistent** if every element of $X$ can be deduced by $\mathcal{F}$ from other elements in $X$. 
**Intuition**

Given a deduction system, it characterizes two possible distinct sets (of provable judgements) according to whether an inductive or a coinductive approach is used.

Let $F$ be a deduction system on a universe $U$ (i.e. a monotone function from $P(U)$ to $P(U)$). A set $X \in P(U)$ is:

- $F$-closed if it contains all the elements that can be deduced by $F$ with hypothesis in $X$.
- $F$-consistent if every element of $X$ can be deduced by $F$ from other elements in $X$.

**Induction and coinduction**

A deduction system

- *inductively* defines the least $F$-closed set
- *coinductively* defines the greatest $F$-consistent set
induction: start from $\emptyset$, add all the consequences of the deduction system, and iterate.

coinduction: start from $\mathcal{U}$, remove all elements that are not consequence of other elements, and iterate.
Induction and coinduction

**induction:** start from $\emptyset$, add all the consequences of the deduction system, and iterate.

**coinduction:** start from $\mathcal{U}$, remove all elements that are not consequence of other elements, and iterate.

**Observation**

In all the (algorithmic, ie without refl and trans) subtyping system met so far, the two coincide. This is not true in general, due to the presence of *self-justifying sets*, that is sets in which the deductions do not start just by axioms.
**Induction and coinduction**

**induction:** start from $\emptyset$, add all the consequences of the deduction system, and iterate.

**coinduction:** start from $\mathcal{U}$, remove all elements that are not consequence of other elements, and iterate.

**Observation**
In all the (algorithmic, ie without refl and trans) subtyping system met so far, the two coincide. This is not true in general, due to the presence of **self-justifying sets**, that is sets in which the deductions do not start just by axioms.

**Example:**

$$
\mathcal{U} = \{a, b, c, d, e, f, g\} \\
\begin{array}{ccccccc}
  a & b & c & d & e & f \\
\hline
  b & c & a & d & e & g
\end{array}
$$
**Induction and coinduction**

**induction:** start from $\emptyset$, add all the consequences of the deduction system, and iterate.

**coinduction:** start from $U$, remove all elements that are not consequence of other elements, and iterate.

**Observation**

In all the (algorithmic, ie without refl and trans) subtyping system met so far, the two coincide. This is not true in general, due to the presence of *self-justifying sets*, that is sets in which the deductions do not start just by axioms.

**Example:**

$$U = \{a, b, c, d, e, f, g\}$$

<table>
<thead>
<tr>
<th></th>
<th>$a$</th>
<th>$b$</th>
<th>$c$</th>
<th>$d$</th>
<th>$e$</th>
<th>$f$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$b$</td>
<td>$c$</td>
<td>$a$</td>
<td>$d$</td>
<td>$e$</td>
<td>$g$</td>
</tr>
</tbody>
</table>

Inductively:

{}
**Induction and coinduction**

**induction:** start from $\emptyset$, add all the consequences of the deduction system, and iterate.

**coinduction:** start from $\mathcal{U}$, remove all elements that are not consequence of other elements, and iterate.

**Observation**

In all the (algorithmic, ie without refl and trans) subtyping system met so far, the two coincide. This is not true in general, due to the presence of **self-justifying sets**, that is sets in which the deductions do not start just by axioms.

**Example:**

\[ \mathcal{U} = \{ a, b, c, d, e, f, g \} \]

\[
\begin{array}{cccccc}
  a & b & c & d & e & f \\
  b & c & a & d & e & g \\
\end{array}
\]

Inductively:

\[ \{ d \} \]
**Induction and coinduction**

**induction:** start from $\emptyset$, add all the consequences of the deduction system, and iterate.

**coinduction:** start from $\mathcal{U}$, remove all elements that are not consequence of other elements, and iterate.

**Observation**

In all the (algorithmic, ie without refl and trans) subtyping system met so far, the two coincide. This is not true in general, due to the presence of *self-justifying sets*, that is sets in which the deductions do not start just by axioms.

**Example:**

$\mathcal{U} = \{a, b, c, d, e, f, g\}$

Inductively:

$\{d, e\}$
**Induction and coinduction**

**induction:** start from $\emptyset$, add all the consequences of the deduction system, and iterate.

**coinduction:** start from $\mathcal{U}$, remove all elements that are not consequence of other elements, and iterate.

**Observation**
In all the (algorithmic, ie without refl and trans) subtyping system met so far, the two coincide. This is not true in general, due to the presence of **self-justifying sets**, that is sets in which the deductions do not start just by axioms.

**Example:**

\[ \mathcal{U} = \{a, b, c, d, e, f, g\} \]

\[
\begin{array}{cccccccc}
  a & b & c & d & e & f \\
  b & c & a & d & e & g \\
\end{array}
\]

Inductively:

\[ \{d, e\} \]
**Induction and coinduction**

**Induction:** start from $\emptyset$, add all the consequences of the deduction system, and iterate.

**Coinduction:** start from $\mathcal{U}$, remove all elements that are not consequence of other elements, and iterate.

---

**Observation**

In all the (algorithmic, ie without refl and trans) subtyping system met so far, the two coincide. This is not true in general, due to the presence of **self-justifying sets**, that is sets in which the deductions do not start just by axioms.

**Example:**

Let $\mathcal{U} = \{a, b, c, d, e, f, g\}$

<table>
<thead>
<tr>
<th>$\mathcal{U}$</th>
<th>${a, b, c, d, e, f, g}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>$b$</td>
<td>$c$</td>
</tr>
<tr>
<td>$c$</td>
<td>$a$</td>
</tr>
<tr>
<td>$d$</td>
<td>$e$</td>
</tr>
<tr>
<td>$e$</td>
<td>$f$</td>
</tr>
<tr>
<td>$f$</td>
<td>$g$</td>
</tr>
</tbody>
</table>

**Inductively:**

$\{d, e\}$

**Coinductively:**

$\{a, b, c, d, e, f, g\} = \mathcal{U}$
**Induction and coinduction**

**induction:** start from $\emptyset$, add all the consequences of the deduction system, and iterate.

**coinduction:** start from $\mathcal{U}$, remove all elements that are not consequence of other elements, and iterate.

**Observation**
In all the (algorithmic, ie without refl and trans) subtyping system met so far, the two coincide. This is not true in general, due to the presence of **self-justifying sets**, that is sets in which the deductions do not start just by axioms.

**Example:**

$\mathcal{U} = \{a, b, c, d, e, f, g\}$

\[
\begin{array}{cccccc}
 a & b & c & d & e & f \\
 b & c & a & d & e & g \\
\end{array}
\]

**Inductively:**
$\{d, e\}$

**Coinductively:**
$\{a, b, c, d, e, f, g\}$
Induction and coinduction

**induction:** start from $\emptyset$, add all the consequences of the deduction system, and iterate.

**coinduction:** start from $\mathcal{U}$, remove all elements that are not consequence of other elements, and iterate.

**Observation**
In all the (algorithmic, ie without refl and trans) subtyping system met so far, the two coincide. This is not true in general, due to the presence of **self-justifying sets**, that is sets in which the deductions do not start just by axioms.

**Example:**
\[
\mathcal{U} = \{a, b, c, d, e, f, g\}
\]

<table>
<thead>
<tr>
<th></th>
<th>$a$</th>
<th>$b$</th>
<th>$c$</th>
<th>$d$</th>
<th>$e$</th>
<th>$f$</th>
<th>$g$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\frac{1}{b}$</td>
<td>$b$</td>
<td></td>
<td>$\frac{1}{c}$</td>
<td>$c$</td>
<td></td>
<td>$\frac{1}{a}$</td>
<td>$a$</td>
</tr>
<tr>
<td>$\frac{1}{d}$</td>
<td></td>
<td>$d$</td>
<td></td>
<td></td>
<td>$\frac{1}{e}$</td>
<td>$e$</td>
<td></td>
</tr>
</tbody>
</table>

Inductively: $\{d, e\}$

Coinductively: $\{a, b, c, d, e, g\}$
Induction and coinduction

**induction:** start from $\emptyset$, add all the consequences of the deduction system, and iterate.

**coinduction:** start from $U$, remove all elements that are not consequence of other elements, and iterate.

**Observation**

In all the (algorithmic, ie without refl and trans) subtyping system met so far, the two coincide. This is not true in general, due to the presence of **self-justifying sets**, that is sets in which the deductions do not start just by axioms.

**Example:**

\[ U = \{a, b, c, d, e, f, g\} \]

Inductively: \[ \{d, e\} \]

Coinductively: \[ \{a, b, c, d, e, g\} \]
**Induction and coinduction**

**induction:** start from $\emptyset$, add all the consequences of the deduction system, and iterate.

**coinduction:** start from $\mathcal{U}$, remove all elements that are not consequence of other elements, and iterate.

**Observation**

In all the (algorithmic, ie without refl and trans) subtyping system met so far, the two coincide. This is not true in general, due to the presence of **self-justifying sets**, that is sets in which the deductions do not start just by axioms.

**Example:**

$\mathcal{U} = \{a, b, c, d, e, f, g\}$

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathcal{U}$</td>
<td>$\mathcal{U}$</td>
<td>$\mathcal{U}$</td>
<td>$\mathcal{U}$</td>
<td>$\mathcal{U}$</td>
<td>$\mathcal{U}$</td>
<td>$\mathcal{U}$</td>
</tr>
<tr>
<td>$a$</td>
<td>$b$</td>
<td>$c$</td>
<td>$d$</td>
<td>$e$</td>
<td>$f$</td>
<td>$g$</td>
</tr>
<tr>
<td>$b$</td>
<td>$c$</td>
<td>$a$</td>
<td>$d$</td>
<td>$e$</td>
<td>$f$</td>
<td>$g$</td>
</tr>
</tbody>
</table>

Inductively: $\{d, e\}$

Coinductively: $\{a, b, c, d, e\}$
Induction and coinduction

**induction:** start from $\emptyset$, add all the consequences of the deduction system, and iterate.

**coinduction:** start from $\mathcal{U}$, remove all elements that are not consequence of other elements, and iterate.

**Observation**

In all the (algorithmic, ie without refl and trans) subtyping system met so far, the two coincide. This is not true in general, due to the presence of **self-justifying sets**, that is sets in which the deductions do not start just by axioms.

**Example:**

\[ \mathcal{U} = \{a, b, c, d, e, f, g\} \]

<table>
<thead>
<tr>
<th>Inductively:</th>
<th>Coinductively:</th>
<th>Self-justifying set:</th>
</tr>
</thead>
<tbody>
<tr>
<td>${d, e}$</td>
<td>${a, b, c, d, e}$</td>
<td>${a, b, c}$</td>
</tr>
</tbody>
</table>
Exercises

1. Let \( \mathcal{U} = \mathbb{Z} \) and take as deduction system all the instances of the rule

\[
\frac{n}{n+1}
\]

for \( n \in \mathbb{Z} \). Which are the sets inductively and coinductively defined by it?

2. Same question but with \( \mathcal{U} = \mathbb{N} \).

3. Same question but with \( \mathcal{U} = \mathbb{N}^2 \) and as deduction system all the rules instance of

\[
\frac{(m, n) \quad (n, o)}{(m, o)}
\]

for \( m, n, o \in \mathbb{N} \).
Why Coinduction for Recursive types?

We want to use $S = \mu X. \text{Int} \to X$ where $T = \mu Y. \text{Even} \to Y$ is expected.
Why Coinduction for Recursive types?

We want to use $S = \mu X.\text{Int} \rightarrow X$ where $T = \mu Y.\text{Even} \rightarrow Y$ is expected.

Use the substitutability interpretation.
Let $e : T$ then $e$:

1. waits for an $\text{Even}$ number,
2. fed by an $\text{Even}$ number returns a function that behaves similarly: (1) wait for an $\text{Even}$ ...
Why Coinduction for Recursive types?

We want to use $S = \mu X. \text{Int} \to X$ where $T = \mu Y. \text{Even} \to Y$ is expected.

Use the substitutability interpretation.

Let $e : T$ then $e$:

1. waits for an $\text{Even}$ number,
2. fed by an $\text{Even}$ number returns a function that behaves similarly: (1) wait for an $\text{Even}$ ...

Now consider $f : S$, then $f$:

1. waits for an $\text{Int}$ number,
2. fed by an $\text{Int}$ (or a $\text{Even}$) number returns a function that behaves similarly: (1) wait for ...
Why Coinduction for Recursive types?

We want to use \( S = \mu X.\text{Int} \rightarrow X \) where \( T = \mu Y.\text{Even} \rightarrow Y \) is expected.

Use the substitutability interpretation.
Let \( e : T \) then \( e \):

1. waits for an \( \text{Even} \) number,
2. fed by an \( \text{Even} \) number returns a function that behaves similarly: (1) wait for an \( \text{Even} \) ...

Now consider \( f : S \), then \( f \):

1. waits for an \( \text{Int} \) number,
2. fed by an \( \text{Int} \) (or a \( \text{Even} \)) number returns a function that behaves similarly: (1) wait for ...

\[ S \leq T \implies \text{Int} \rightarrow S \leq \text{Even} \rightarrow T \implies S \leq T \wedge \text{Even} \leq \text{Int} \]

\( S \) and \( T \) are in subtyping relation because their infinite expansions are in subtyping relation.
This is exactly the proof we saw at the beginning:

\[
\begin{align*}
\text{ARROW} & : \quad \text{Even} \leq \text{Int} \quad \frac{\mu X. \text{Int} \to X \leq \mu Y. \text{Even} \to Y}{\text{Int} \to (\mu X. \text{Int} \to X) \leq \text{Even} \to (\mu Y. \text{Even} \to Y)} \\
\text{UNFOLD RIGHT} & : \quad \frac{\text{Int} \to (\mu X. \text{Int} \to X) \leq \text{Even} \to (\mu Y. \text{Even} \to Y)}{\mu X. \text{Int} \to X \leq \mu Y. \text{Even} \to Y} \\
\text{UNFOLD LEFT} & : \quad \frac{\mu X. \text{Int} \to X \leq \mu Y. \text{Even} \to Y}{\frac{S}{\text{S} \leq \frac{T}{T}}}
\end{align*}
\]
This is exactly the proof we saw at the beginning:

\[
\begin{align*}
\text{ARROW} & \quad \frac{\text{Even } \leq \text{ Int}}{\mu X. \text{Int} \rightarrow X \leq \mu Y. \text{Even} \rightarrow Y} \\
\text{UNFOLD RIGHT} & \quad \frac{\text{Int} \rightarrow (\mu X. \text{Int} \rightarrow X) \leq \text{Even} \rightarrow (\mu Y. \text{Even} \rightarrow Y)}{\text{Int} \rightarrow (\mu X. \text{Int} \rightarrow X) \leq \mu Y. \text{Even} \rightarrow Y} \\
\text{UNFOLD LEFT} & \quad \frac{\mu X. \text{Int} \rightarrow X \leq \mu Y. \text{Even} \rightarrow Y}{\mu X. \text{Int} \rightarrow X \leq \mu Y. \text{Even} \rightarrow Y}
\end{align*}
\]

**Coinduction**

\( S \leq T \) is not an axiom but \( \{S \leq T, \text{Even } \leq \text{ Int}\} \) is a **self-justifying set**.
This is exactly the proof we saw at the beginning:

\[
\begin{align*}
\text{Even} \leq \text{Int} & \quad \frac{\mu X. \text{Int} \to X \leq \mu Y. \text{Even} \to Y}{\text{Int} \to (\mu X. \text{Int} \to X) \leq \text{Even} \to (\mu Y. \text{Even} \to Y)} \\
\text{Unfold Right} & \quad \frac{\text{Int} \to (\mu X. \text{Int} \to X) \leq \mu Y. \text{Even} \to Y}{\mu X. \text{Int} \to X \leq \mu Y. \text{Even} \to Y}
\end{align*}
\]

Coinduction

\[S \leq T\] is not an axiom but \(\{S \leq T, \text{Even} \leq \text{Int}\}\) is a self-justifying set.

Observation:

1. The deduction above shows why a specific rule for \(\mu\) is useless (apply consecutively the two unfold rules).
2. If we added reflexivity and/or transitivity rules, then \(\mathcal{U}\) would be \(\mathcal{F}\)-consistent (cf. the third exercise on slide 61).
A naive implementation of the Amadio-Cardelli algorithm is exponential (why?). If we “thread” the computation of the memoization environments we obtain a quadratic complexity. This is done as follows:

\[
\text{subtype}(A, S, T) = \begin{cases} 
A & \text{if } (S, T) \in A \\
\text{fail} & \text{else} 
\end{cases}
\]
A naive implementation of the Amadio-Cardelli algorithm is exponential (why?). If we “thread” the computation of the memoization environments we obtain a quadratic complexity. This is done as follows:

\[
\text{subtype}(A, S, T) = \begin{cases} 
\text{if } (S, T) \in A \text{ then } A \text{ else } \\
\text{let } A_0 = A \cup \{(S, T)\} \in 
\end{cases}
\]
A naive implementation of the Amadio-Cardelli algorithm is exponential (why?). If we “thread” the computation of the memoization environments we obtain a quadratic complexity. This is done as follows:

\[
\text{subtype}(A, S, T) = \begin{cases} 
A & \text{if } (S, T) \in A \\
\text{else} & \\
\text{let } A_0 = A \cup \{(S, T)\} \text{ in} \\
\text{if } T = \text{Any} \text{ then } A_0 
\end{cases}
\]
A naive implementation of the Amadio-Cardelli algorithm is exponential (why?). If we “thread” the computation of the memoization environments we obtain a quadratic complexity. This is done as follows:

\[
\text{subtype}(A, S, T) = \begin{cases} 
\text{if } (S, T) \in A \text{ then } A \text{ else} \\
\text{let } A_0 = A \cup \{ (S, T) \} \text{ in} \\
\text{if } T = \text{Any} \text{ then } A_0 \\
\text{else if } S = S_1 \times S_2 \text{ and } T = T_1 \times T_2 \text{ then} \\
\text{subtype(} \text{subtype}(A_0, S_1, T_1), S_2, T_2 \text{)}
\end{cases}
\]
A naive implementation of the Amadio-Cardelli algorithm is exponential (why?). If we “thread” the computation of the memoization environments we obtain a quadratic complexity. This is done as follows:

\[ \text{subtype}(A, S, T) = \begin{cases} \text{if } (S, T) \in A \text{ then } A \text{ else} \\ \text{let } A_0 = A \cup \{(S, T)\} \text{ in} \\ \text{if } T = \text{Any} \text{ then } A_0 \\ \text{else if } S = S_1 \times S_2 \text{ and } T = T_1 \times T_2 \text{ then} \\ \text{subtype}(\text{subtype}(A_0, S_1, T_1), S_2, T_2) \\ \text{else if } S = S_1 \rightarrow S_2 \text{ and } T = T_1 \rightarrow T_2 \text{ then} \\ \text{subtype}(\text{subtype}(A_0, T_1, S_1), S_2, T_2) \end{cases} \]
A naive implementation of the Amadio-Cardelli algorithm is exponential (why?). If we “thread” the computation of the memoization environments we obtain a quadratic complexity. This is done as follows:

\[
\text{subtype}(A, S, T) = \begin{cases} 
\text{if } (S, T) \in A \text{ then } A \text{ else} \\
\text{let } A_0 = A \cup \{(S, T)\} \text{ in} \\
\text{if } T = \text{Any} \text{ then } A_0 \\
\text{else if } S = S_1 \times S_2 \text{ and } T = T_1 \times T_2 \text{ then} \\
\quad \text{subtype(subtype}(A_0, S_1, T_1), S_2, T_2) \\
\text{else if } S = S_1 \rightarrow S_2 \text{ and } T = T_1 \rightarrow T_2 \text{ then} \\
\quad \text{subtype}(\text{subtype}(A_0, T_1, S_1), S_2, T_2) \\
\text{else if } T = \mu X. T_1 \text{ then} \\
\quad \text{subtype}(A_0, S, T_1[\mu X. T_1/X])
\end{cases}
\]
A naive implementation of the Amadio-Cardelli algorithm is exponential (why?). If we “thread” the computation of the memoization environments we obtain a quadratic complexity. This is done as follows:

\[
\text{subtype}(A, S, T) = \begin{cases} 
\text{if } (S, T) \in A \text{ then } A \text{ else} \\
\text{let } A_0 = A \cup \{(S, T)\} \text{ in} \\
\text{if } T = \text{Any} \text{ then } A_0 \\
\text{else if } S = S_1 \times S_2 \text{ and } T = T_1 \times T_2 \text{ then} \\
\text{subtype}(\text{subtype}(A_0, S_1, T_1), S_2, T_2) \\
\text{else if } S = S_1 \rightarrow S_2 \text{ and } T = T_1 \rightarrow T_2 \text{ then} \\
\text{subtype}(\text{subtype}(A_0, T_1, S_1), S_2, T_2) \\
\text{else if } T = \mu X.T_1 \text{ then} \\
\text{subtype}(A_0, S, T_1[\mu X.T_1 / X]) \\
\text{else if } S = \mu X.S_1 \text{ then} \\
\text{subtype}(A_0, S_1[\mu X.S_1 / X], T)
\end{cases}
\]
A naive implementation of the Amadio-Cardelli algorithm is exponential (why?). If we “thread” the computation of the memoization environments we obtain a quadratic complexity. This is done as follows:

\[
\text{subtype}(A, S, T) = \begin{cases} 
\text{if} \ (S, T) \in A \ \text{then} \ A & \text{else} \\
\text{let} \ A_0 = A \cup \{(S, T)\} \ \text{in} \\
\text{if} \ T = \text{Any} \ \text{then} \ A_0 \\
\text{else if} \ S = S_1 \times S_2 \ \text{and} \ T = T_1 \times T_2 \ \text{then} \\
\text{subtype(}\text{subtype}(A_0, S_1, T_1), S_2, T_2) \\
\text{else if} \ S = S_1 \rightarrow S_2 \ \text{and} \ T = T_1 \rightarrow T_2 \ \text{then} \\
\text{subtype(}\text{subtype}(A_0, T_1, S_1), S_2, T_2) \\
\text{else if} \ T = \mu X. T_1 \ \text{then} \\
\text{subtype}(A_0, S, T_1[\mu X. T_1 / X]) \\
\text{else if} \ S = \mu X. S_1 \ \text{then} \\
\text{subtype}(A_0, S_1[\mu X. S_1 / X], T) \\
\text{else} \ \text{fail}
\end{cases}
\]
Compare the previous algorithm with the Amadio-Cardelli algorithm:

\[ A \vdash S \leq T \quad (S, T) \in A \]

\[ A \vdash S \leq \text{Any} \quad (S, \text{Any}) \notin A \]

\[ \begin{align*}
A' \vdash S_1 \leq T_1 \\
A' \vdash S_2 \leq T_2 \\
\hline
A \vdash S_1 \times S_2 \leq T_1 \times T_2 
\end{align*} \]

\[ A' = A \cup (S_1 \times S_2, T_1 \times T_2); A \neq A' \]

\[ \begin{align*}
A' \vdash T_1 \leq S_1 \\
A' \vdash S_2 \leq T_2 \\
\hline
A \vdash S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2 
\end{align*} \]

\[ A' = A \cup (S_1 \rightarrow S_2, T_1 \rightarrow T_2); A \neq A' \]

\[ \begin{align*}
A' \vdash S[\mu X.S/X] \leq T \\
\hline
A \vdash \mu X.S \leq T 
\end{align*} \]

\[ A' = A \cup (\mu X.S, T); A \neq A'; T \neq \text{Any} \]

\[ \begin{align*}
A' \vdash S \leq T[\mu X.T/X] \\
\hline
A \vdash S \leq \mu X.T 
\end{align*} \]

\[ A' = A \cup (S, \mu X.T); A \neq A'; S \neq \mu Y.U \]
They both check containment in the relation coinductively defined by:

\[
\begin{align*}
\text{TOP} & \quad T \leq \text{Any} \\
\text{PROD} & \quad S_1 \leq T_1 \quad S_2 \leq T_2 \\
& \quad S_1 \times S_2 \leq T_1 \times T_2 \\
\text{ARROW} & \quad T_1 \leq S_1 \quad S_2 \leq T_2 \\
& \quad S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2 \\
\text{UNFOLD LEFT} & \quad S[\mu X . S/X] \leq T \\
& \quad \mu X . S \leq T \\
\text{UNFOLD RIGHT} & \quad S \leq T[\mu X . T/X] \\
& \quad S \leq \mu X . T
\end{align*}
\]

But the former is far more efficient.
Outline

4 Simple Types

5 Recursive Types

6 Bibliography

Parametric polymorphism
Outline

7 Introduction

8 Hindley-Milner System

9 Inference algorithm
Outline

Introduction

Hindley-Milner System

Inference algorithm
Monomorphic calculus

**Types** \[ T ::= \text{Bool} | \text{Int} | \text{Real} | \ldots \] basic types
| \[ T \rightarrow T \] function types

**Terms** \[ a, b ::= \text{true} | \text{false} | 1 | 2 | \ldots \] constants
| \[ x \] variable
| \[ ab \] application
| \[ \lambda x:T.a \] abstraction
| \[ \text{let } x:T = a \text{ in } b \] let

\[
\begin{align*}
\Gamma, x:S & \vdash a : T & \Gamma \vdash a : S \rightarrow T & \Gamma \vdash b : S \\
\Gamma \vdash x : \Gamma(x) & \quad \Gamma \vdash \lambda x:S.a : S \rightarrow T & \Gamma \vdash ab : T \\
\Gamma \vdash a : S & \Gamma, x:S \vdash b : T & \Gamma \vdash \text{let } x:S = a \text{ in } b : T
\end{align*}
\]
It is a pity to use the identity function just with a single type.

\[
\text{let } f : \text{Int} \to \text{Int} = \lambda x : \text{Int}. x \text{ in } b
\]

In particular, if we get rid of type annotations we see that the identity function can be given several different types.

\[
\begin{align*}
\Gamma \vdash x : \Gamma(x) & \quad \Gamma, x : S \vdash a : T & \quad \Gamma \vdash a : S \rightarrow T & \quad \Gamma \vdash b : S \\
\Gamma \vdash \lambda x. a : S \rightarrow T & \quad \Gamma \vdash ab : T \\
\Gamma \vdash a : S & \quad \Gamma, x : S \vdash b : T \\
\Gamma \vdash \text{let } x = a \text{ in } b : T
\end{align*}
\]

In particular, \( \lambda x. x \) can be given all the types of the form \( T \rightarrow T \) for every \( T \).
Parametric polymorphism

We extend the syntax of types

\[
Types \quad T ::=
\begin{array}{l}
\text{Bool} | \text{Int} | \text{Real} | \ldots \\
T \to T \\
\alpha \\
\forall \alpha. T
\end{array}
\]

basic types

function types

type variables

polymorphic types

We add to the previous rules these two rules

\[
\Gamma \vdash a : T \quad \alpha \not\in \text{fv}(\Gamma) \\
\frac{}{\Gamma \vdash a : \forall \alpha. T}
\]

\[
\Gamma \vdash a : \forall \alpha. T \\
\frac{}{\Gamma \vdash a : T[S/\alpha]}
\]

The resulting system is called System F (Girard/Reynolds)
We can for instance derive

\[ \lambda x.xx : (\forall \alpha. \alpha \rightarrow \alpha) \rightarrow (\forall \alpha. \alpha \rightarrow \alpha) \]

and supposing we have pairs:

\[ \text{let } f = \lambda x.x \text{ in } (f 3, f \text{true}) : \text{Int} \times \text{Bool} \]
Remark

The condition $\alpha \notin \text{fv}(\Gamma)$ in the rule

$$
\Gamma \vdash a : T \quad \alpha \notin \text{fv}(\Gamma)
$$

$$
\Gamma \vdash a : \forall \alpha . T
$$

is crucial ... without it we can derive

$$
\begin{align*}
\Gamma \vdash x : \alpha &
\quad \Gamma \vdash x : \alpha \\
\Gamma \vdash x : \forall \alpha . \alpha &
\quad \Gamma \vdash \lambda x . x : \alpha \to (\forall \alpha . \alpha)
\end{align*}
$$

and therefore type, for instance, $(\lambda x . x)12$ with any type we wish
For terms without type annotations the problems:

- **type inference**: given an expression $a$ find if there exists a type $T$ such that $a : T$
- **type checking**: given an expression $a$ and a type $T$ check whether $a : T$ holds

are both undecidable

(J. B. Wells. *Typability and type checking in the second-order lambda-calculus are equivalent and undecidable*, 1994.)
Bad news

For terms without type annotations the problems:

- **type inference**: given an expression \( a \) find if there exists a type \( T \) such that \( a : T \)

- **type checking**: given and expression \( a \) and a type \( T \) check whether \( a : T \) holds

are both undecidable

(J. B. Wells. *Typability and type checking in the second-order lambda-calculus are equivalent and undecidable*, 1994.)

**Solution 1**: use explicit type abstractions and instantiations (e.g., generics)

**Solution 2**: restrict the power of the system (e.g., Hindley-Milner)
Bad news

For terms without type annotations the problems:

- **type inference**: given an expression \( a \) find if there exists a type \( T \) such that \( a : T \)

- **type checking**: given and expression \( a \) and a type \( T \) check whether \( a : T \) holds

are both undecidable

(J. B. Wells. *Typability and type checking in the second-order lambda-calculus are equivalent and undecidable*, 1994.)

**Solution 1**: use explicit type abstractions and instantiations (e.g., generics)

**Solution 2**: restrict the power of the system (e.g., Hindley-Milner)

---

**Hindley-Milner**

We restrict the power of System F to have decidable type inference and type checking

(used in OCaml, SML, Haskell, etc ...)
Outline

7 Introduction

8 Hindley-Milner System

9 Inference algorithm
Hindley-Milner System

The quantification can only be prenex:

\[
\text{Types} \quad T ::= \text{Bool} \mid \text{Int} \mid \text{Real} \mid \ldots \quad \text{basic types}
\]

\[
\quad \mid T \rightarrow T \quad \text{function types}
\]

\[
\quad \mid \alpha \quad \text{type variables}
\]

\[
\text{Schemas} \quad \sigma ::= T \quad \text{type}
\]

\[
\quad \mid \forall \alpha. \sigma \quad \text{schema}
\]

A type environment $\Gamma$ now maps variable to schemas, and typing judgement have the form $\Gamma \vdash a : \sigma$
The following types (schemas) are ok:

\[ \forall \alpha. \alpha \rightarrow \alpha \]
\[ \forall \alpha. \forall \beta. (\alpha \times \beta) \rightarrow \alpha \]
\[ \forall \alpha. \text{Bool} \rightarrow \alpha \rightarrow \alpha \rightarrow \alpha \]
\[ \forall \alpha. (\alpha \rightarrow \alpha) \rightarrow \alpha \]

but the following type is not longer allowed:

\[ (\forall \alpha. \alpha \rightarrow \alpha) \rightarrow (\forall \alpha. \alpha \rightarrow \alpha) \]
Hindley-Milner System

\[ \Gamma \vdash x : \Gamma(x) \quad \Gamma, x : S \vdash a : T \quad \Gamma \vdash \lambda x.a : S \to T \quad \Gamma \vdash a : S \to T \quad \Gamma \vdash b : S \quad \Gamma \vdash ab : T \]

\[ \Gamma \vdash a : \sigma_1 \quad \Gamma, x : \sigma_1 \vdash b : \sigma_2 \quad \Gamma \vdash a : T \quad \alpha \notin fv(\Gamma) \quad \Gamma \vdash a : \forall \alpha. T \quad \Gamma \vdash a : T[S/\alpha] \]

\[ \Gamma \vdash \text{let } x = a \text{ in } b : \sigma_2 \]

G. Castagna (CNRS)
Hindley-Milner System

Notice that the rule for let is the (only) rule that introduce a polymorphic type in the type environment.

$$\Gamma \vdash a : \sigma_1 \quad \Gamma, x : \sigma_1 \vdash b : \sigma_2$$

$$\Gamma \vdash \text{let } x = a \ \text{in } b : \sigma_2$$

Thanks to this we can for instance type

$$\text{let } f = \lambda x. x \ \text{in } (f f)(f 1)$$

with $f : \forall \alpha. \alpha \rightarrow \alpha$ in the context to type $(f f)(f 1)$ in order to use three times the instantiation rule for the type schema:

$$f : \forall \alpha. \alpha \rightarrow \alpha \vdash f : \forall \alpha. \alpha \rightarrow \alpha$$

$$f : \forall \alpha. \alpha \rightarrow \alpha \vdash f : (\alpha \rightarrow \alpha)[T/\alpha]$$

where $T$ is respectively for each occurrence of $f$, $(\text{Int} \rightarrow \text{Int}) \rightarrow \text{Int} \rightarrow \text{Int}$, $\text{Int} \rightarrow \text{Int}$, and $\text{Int}$. 
On the contrary the rule for abstractions does not introduce in the environment a schema, but just a type

\[ \Gamma, x : S \vdash a : T \]

\[ \Gamma \vdash \lambda x. a : S \rightarrow T \]

otherwise \( S \rightarrow T \) would not be well formed.

In particular,

\[ \lambda x. xx \]

is no longer typeable, while

\[ \text{let } f = \lambda x. x \text{ in } ff \]

is still typeable.
Hindley-Milner Algorithm

The system is not syntax directed because of the following two rules apply to any expression:

\[
\Gamma \vdash a : T \quad \alpha \not\in \text{fv}(\Gamma) \\
\adjustfrac{\Gamma \vdash a : \forall \alpha. T}{\Gamma \vdash a : T[S/\alpha]}
\]
Hindley-Milner syntax-directed system

$$\Gamma, x : S \vdash a : T \quad \Gamma \vdash \lambda x. a : S \rightarrow T \quad \Gamma \vdash b : S \quad \Gamma \vdash ab : T \quad \Gamma \vdash a : S \rightarrow T \quad \Gamma, x : \text{Gen}(S, \Gamma) \vdash b : T \quad \Gamma \vdash \text{let } x = a \text{ in } b : T$$
Hindley-Milner syntax-directed system

\[
\begin{align*}
\Gamma, x : S &\vdash a : T \\
\therefore \Gamma \vdash \lambda x. a : S \rightarrow T \\
\Gamma \vdash a : S \rightarrow T &\quad \Gamma \vdash b : S \\
\therefore \Gamma \vdash ab : T
\end{align*}
\]

Where

\[
T \sqsubseteq \forall \alpha_1 \ldots \forall \alpha_n. S \iff \exists S_1, \ldots, S_n \text{ such that } T = S[S_1/\alpha_1 \ldots S_n/\alpha_n]
\]

and

\[
\text{Gen}(S, \Gamma) = \forall \alpha_1 \ldots \forall \alpha_n. S \text{ where } \{\alpha_1, \ldots, \alpha_n\} = \text{fv}(S) \setminus \text{fv}(\Gamma)
\]
Hindley-Milner syntax-directed system

\[
\begin{align*}
\Gamma, \, x : S & \vdash a : T \\
\Gamma & \vdash \lambda x. a : S \to T \\
\Gamma & \vdash a : S \to T \\
\Gamma & \vdash b : S \\
\Gamma & \vdash ab : T
\end{align*}
\]

\[
\begin{align*}
T & \sqsubseteq \Gamma(x) \\
\Gamma & \vdash a : S \\
\Gamma & \vdash x : \text{Gen}(S, \Gamma) \\
\Gamma & \vdash b : T \\
\Gamma & \vdash \text{let } x = a \text{ in } b : T
\end{align*}
\]

Where

\[
T \sqsubseteq \forall \alpha_1 \ldots \forall \alpha_n. S \iff \exists S_1, \ldots, S_n \text{ such that } T = S[S_1/\alpha_1 \ldots S_n/\alpha_n]
\]

and

\[
\text{Gen}(S, \Gamma) = \forall \alpha_1 \ldots \forall \alpha_n. S \text{ where } \{\alpha_1, \ldots, \alpha_n\} = \text{fv}(S) \setminus \text{fv}(\Gamma)
\]
State: a current substitution $\phi$ and an infinite set of fresh variables $V$

\[
\text{fresh} = \text{do } \alpha \in V \\
\text{do } V := V \setminus \{\alpha\} \\
\text{return } \alpha
\]

\[
W(\Gamma \vdash x) = \text{let } \forall \alpha_1, \ldots, \alpha_n. T \leftarrow \Gamma(x) \\
\text{do } \beta_1, \ldots, \beta_n \leftarrow \text{fresh, ..., fresh} \\
\text{return } T[\beta_1/\alpha_1, \ldots, \beta_n/\alpha_n]
\]

\[
W(\Gamma \vdash \lambda x.a) = \text{do } \alpha \leftarrow \text{fresh} \\
\text{do } T \leftarrow W(\Gamma, x : \alpha \vdash a) \\
\text{return } \alpha \rightarrow T
\]

\[
W(\Gamma \vdash ab) = \text{do } T \leftarrow W(\Gamma \vdash a) \\
\text{do } S \leftarrow W(\Gamma \vdash b) \\
\text{do } \alpha \leftarrow \text{fresh} \\
\text{do } \phi := \text{mgu}(\phi(T), \phi(S \rightarrow \alpha)) \circ \phi \\
\text{return } \alpha
\]

\[
W(\Gamma \vdash \text{let } x = a \text{ in } b) = \text{do } S \leftarrow W(\Gamma \vdash a) \\
\text{do } \sigma \leftarrow \text{Gen}(\phi(S), \phi(\Gamma)) \\
\text{return } W(\Gamma, x : \sigma \vdash b)
\]
Most General Unifier

\[
\begin{align*}
\text{mgu}(\emptyset) &= \text{id} \\
\text{mgu}(\{(\alpha, \alpha)\} \cup C) &= \text{mgu}(C) \\
\text{mgu}(\{(\alpha, T)\} \cup C) &= \text{mgu}(C[T/\alpha]) \circ [T/\alpha] \text{ if } \alpha \text{ not free in } T \\
\text{mgu}(\{(T, \alpha)\} \cup C) &= \text{mgu}(C[T/\alpha]) \circ [T/\alpha] \text{ if } \alpha \text{ not free in } T \\
\text{mgu}(\{(S_1 \rightarrow S_2, T_1 \rightarrow T_2)\} \cup C) &= \text{mgu}(\{(S_1, T_1), (S_2, T_2)\} \cup C)
\end{align*}
\]

In all the other cases \text{mgu} fails
Ad-Hoc Polymorphism
Outline

10 Set-theoretic types

11 Semantic Subtyping

12 Application to a language.

13 Adding Parametric Polymorphism: the Types

14 Adding Parametric Polymorphism: the Language
Outline

10 Set-theoretic types

11 Semantic Subtyping

12 Application to a language.

13 Adding Parametric Polymorphism: the Types

14 Adding Parametric Polymorphism: the Language
Set-theoretic types

We consider the following possibly recursive types:

\[ T ::= \text{Bool} \mid \text{Int} \mid \text{Any} \mid (T, T) \mid T \lor T \mid T \land T \mid \text{not}(T) \mid T \rightarrow T \]

Useful for:

1. XML types
2. Precise typing of pattern matching
3. Overloaded functions
4. Mixins
5. General programming paradigms

Let us see each point more in detail

Note: henceforward I will sometimes use \( T_1 \mid T_2 \) to denote \( T_1 \lor T_2 \)
1. XML types

```xml
<?xml version="1.0"?>
<!DOCTYPE biblio [
<!ELEMENT biblio (book*)>
<!ELEMENT book (title, (author+)|(editor+), price?)>
<!ELEMENT title (#PCDATA)>
<!ELEMENT author (#PCDATA)>
<!ELEMENT editor (#PCDATA)>
<!ELEMENT price (#PCDATA)>
]
```

Can be encoded with union and recursive types

```plaintext
type Biblio = ('biblio,X)
type X = (Book,X)\lor 'nil

type Book = ('book,(Title, Y\lor Z))
type Y = (Author,Y\lor (Price, 'nil)\lor 'nil)
type Z = (Editor,Z\lor (Price, 'nil)\lor 'nil)

type Title = ('title,String)
type Author = ('author,String)
type Editor = ('editor,String)
type Price = ('price,String)
```
Consider the following pattern matching expression

\[
\text{match } e \text{ with } p_1 \rightarrow e_1 \mid p_2 \rightarrow e_2
\]

where patterns are defined as follows:

\[
p ::= x \mid (p, p) \mid p|p \mid p\&p
\]
Consider the following pattern matching expression:

\[
\text{match } e \text{ with } p_1 \rightarrow e_1 \mid p_2 \rightarrow e_2
\]

where patterns are defined as follows:

\[
p ::= x \mid (p, p) \mid p | p \mid p \& p
\]

If we interpret types as set of values

\[
t = \{ v \mid v \text{ is a value of type } t \}
\]

then the set of all values that match a pattern is a type

\[
\llbracket p \rrbracket = \{ v \mid v \text{ is a value that matches } p \}
\]

\[
\begin{align*}
\llbracket x \rrbracket &= \text{Any} \\
\llbracket (p_1, p_2) \rrbracket &= \langle \llbracket p_1 \rrbracket, \llbracket p_2 \rrbracket \rangle \\
\llbracket p_1 | p_2 \rrbracket &= \llbracket p_1 \rrbracket \lor \llbracket p_2 \rrbracket \\
\llbracket p_1 \& p_2 \rrbracket &= \llbracket p_1 \rrbracket \& \llbracket p_2 \rrbracket
\end{align*}
\]
Boolean type connectives are needed to *type pattern matching*:
Boolean type connectives are needed to type pattern matching:

\[
\text{match } e \text{ with } p_1 \rightarrow e_1 \mid p_2 \rightarrow e_2
\]
2. Precise typing of pattern matching (II)

Boolean type connectives are needed to type pattern matching:

\[
\text{match } e \text{ with } p_1 \rightarrow e_1 \mid p_2 \rightarrow e_2
\]

Suppose that \( e : T \) and let us write \( T_1 \setminus T_2 \) for \( T_1 \& \neg(T_2) \)
Precise typing of pattern matching (II)

Boolean type connectives are needed to type pattern matching:

match $e$ with $p_1 \rightarrow e_1 \mid p_2 \rightarrow e_2$

Suppose that $e : T$ and let us write $T_1 \setminus T_2$ for $T_1 \& \neg(T_2)$

- To infer the type $T_1$ of $e_1$ we need $T \& \{p_1\}$;

Formally:

$\Gamma \vdash e : T \quad \Gamma, T \& \{p_1\} \vdash e_1 : T_1 \quad \Gamma, T \setminus \{p_1\} \vdash e_2 : T_2$

where $T / p$ is the type environment for the capture variables in $p$ when the pattern is matched against values in $T$. (e.g., $(\text{Int,Int}) / (x,y)$ is $x : \text{Int} \lor \text{Bool}$, $y : \text{Int} \lor \text{Char}$)
2. Precise typing of pattern matching (II)

Boolean type connectives are needed to type pattern matching:

\[
\text{match } e \text{ with } p_1 \rightarrow e_1 \mid p_2 \rightarrow e_2
\]

Suppose that \( e : T \) and let us write \( T_1 \setminus T_2 \) for \( T_1 \& \text{not}(T_2) \):

- To infer the type \( T_1 \) of \( e_1 \) we need \( T \& \| p_1 \|; \)
- To infer the type \( T_2 \) of \( e_2 \) we need \( (T \setminus \| p_1 \|) \& \| p_2 \|; \)
2. Precise typing of pattern matching (II)

Boolean type connectives are needed to type pattern matching:

\[
\text{match } e \text{ with } p_1 \rightarrow e_1 \mid p_2 \rightarrow e_2
\]

Suppose that \( e : T \) and let us write \( T_1 \setminus T_2 \) for \( T_1 \& \text{not}(T_2) \)

- To infer the type \( T_1 \) of \( e_1 \) we need \( T \& \{p_1\} \);
- To infer the type \( T_2 \) of \( e_2 \) we need \( (T \setminus \{p_1\}) \& \{p_2\} \);
- The type of the match expression is \( T_1 \lor T_2 \).
2. Precise typing of pattern matching (II)

Boolean type connectives are needed to type pattern matching:

\[
\text{match } e \text{ with } p_1 \rightarrow e_1 \mid p_2 \rightarrow e_2
\]

Suppose that \( e : T \) and let us write \( T_1 \setminus T_2 \) for \( T_1 \& \neg(T_2) \)

- To infer the type \( T_1 \) of \( e_1 \) we need \( T \& \{ p_1 \} \);  
- To infer the type \( T_2 \) of \( e_2 \) we need \( (T \setminus \{ p_1 \}) \& \{ p_2 \} \);  
- The type of the match expression is \( T_1 \lor T_2 \).  
- Pattern matching is exhaustive if \( T \leq \{ p_1 \} \lor \{ p_2 \} \);
Boolean type connectives are needed to type pattern matching:

\[
\text{match } e \text{ with } p_1 \rightarrow e_1 | p_2 \rightarrow e_2
\]

Suppose that \( e : T \) and let us write \( T_1 \setminus T_2 \) for \( T_1 \& \neg (T_2) \):

- To infer the type \( T_1 \) of \( e_1 \) we need \( T \& \perp p_1\perp \);
- To infer the type \( T_2 \) of \( e_2 \) we need \( (T \setminus \perp p_1\perp ) \& \perp p_2\perp \);
- The type of the match expression is \( T_1 \lor T_2 \).
- Pattern matching is exhaustive if \( T \leq \perp p_1\perp \lor \perp p_2\perp \);
2. Precise typing of pattern matching (II)

Boolean type connectives are needed to type pattern matching:

\[
\text{match } e \text{ with } p_1 \rightarrow e_1 \mid p_2 \rightarrow e_2
\]

Suppose that \( e : T \) and let us write \( T_1 \setminus T_2 \) for \( T_1 \& \text{not}(T_2) \)

- To infer the type \( T_1 \) of \( e_1 \) we need \( T \& \not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!\not\!
3. Overloaded functions

Intersection types are useful to type overloaded functions (in the Go language):

```go
package main
import "fmt"
func Opposite (x interface{}) interface{} {
    var res interface{}
    switch value := x.(type) {
    case bool:
        res = (!value)       // x has type bool
    case int:
        res = (-value)      // x has type int
    }
    return res
}

func main() { fmt.Println(Opposite(3) , Opposite(true)) }
```

In Go `Opposite` has type `Any-->Any` (every value has type `interface{}`). Better type with intersections `Opposite:  (Int-->Int) & (Bool-->Bool)`
3. Overloaded functions

Intersection types are useful to type overloaded functions (in the Go language):

```go
package main
import "fmt"
func Opposite (x interface{}) interface{} {
    var res interface{}
    switch value := x.(type) {
    case bool:
        res = (!value) // x has type bool
    case int:
        res = (-value) // x has type int
    }
    return res
}
func main() { fmt.Println(Opposite(3) , Opposite(true)) }
```

In Go `Opposite` has type `Any-->Any` (every value has type `interface{}`). Better type with intersections `Opposite: (Int-->Int) & (Bool-->Bool)`

Intersections can also to give a more refined description of standard functions:

```go
func Successor(x int) { return(x+1) }
```

which could be typed as `Successor: (Odd-->Even) & (Even-->Odd)`
Exercise:

1. What is the type returned by

   ```ocaml
   let foo = function
       | ('A,'B) -> true
       | ('B,'A) -> false
   ``

   and what is the problem?

2. Which type could we give if we had full-fledged union types?

3. Give an intersection type that refines the previous type.
Exercise:

1. What is the type returned by

   let foo = function
     | ('A,'B) -> true
     | ('B,'A) -> false

   and what is the problem?

   [< 'A | 'B ] * [< 'A | 'B ] -> bool thus foo( 'A , 'A) fails

2. Which type could we give if we had full-fledged union types?

3. Give an intersection type that refines the previous type
Exercise:

1. What is the type returned by

```ocaml
let foo = function
    | ('A,'B) -> true
    | ('B,'A) -> false
```

and what is the problem?

```ocaml
[< 'A | 'B ] * [< 'A | 'B ] -> bool thus foo( 'A , 'A) fails
```

2. Which type could we give if we had full-fledged union types?

```ocaml
('A * 'B )| ( 'B * 'A) -> bool
```

3. Give an intersection type that refines the previous type
Exercise:

1. What is the type returned by

   ```ocaml
   let foo = function
       | ('A,'B) -> true
       | ('B,'A) -> false
   ```

   and what is the problem?

   ```ocaml
   [<'A | 'B] * [<'A | 'B] -> bool
   ```

   thus `foo('A,'A)` fails

2. Which type could we give if we had full-fledged union types?

   ```ocaml
   ('A * 'B) | ('B * 'A) -> bool
   ```

3. Give an intersection type that refines the previous type

   ```ocaml
   (('A * 'B) -> true) & (('B * 'A) -> false)
   ```

You can try it on http://www.cduce.org/ocaml/bi
4. Typing of Mixins

Intersection types are used in Microsoft’s Typescript to type mixins.

```typescript
function extend<T, U>(first: T, second: U): T & U {
    /* <T> exp is a type cast (equivalent: exp as T) */
    let result = <T & U>{};
    for (let id in first) {
        (<any>result)[id] = (<any>first)[id];
    }
    for (let id in second) {
        if (!result.hasOwnProperty(id)) {
            (<any>result)[id] = (<any>second)[id];
        }
    }
    return result;
}

class Person {
    constructor(public name: string) { }
}

interface Loggable {
    log(): void;
}

class ConsoleLogger implements Loggable {
    log() { ... }
}

var jim = extend(new Person("Jim"), new ConsoleLogger());
var n = jim.name;
jim.log();
```
5. General programming paradigms

Consider red-black trees. Recall that they must satisfy 4 invariants.

1. the root of the tree is black
2. the leaves of the tree are black
3. no red node has a red child
4. every path from root to a leaf contains the same number of black nodes
5. General programming paradigms

Consider red-black trees. Recall that they must satisfy 4 invariants.

1. the root of the tree is black
2. the leaves of the tree are black
3. no red node has a red child
4. every path from root to a leaf contains the same number of black nodes

The key of Okasaki’s insertion is the function $\text{balance}$ which transforms an unbalanced tree, into a valid red-black tree (as long as $a$, $b$, $c$, and $d$ are valid):

![Diagram of red-black tree transformations]

In ML we need GADTs to enforce the invariants.
5. General programming paradigms

Consider red-black trees. Recall that they must satisfy 4 invariants:

1. the root of the tree is black
2. the leaves of the tree are black
3. no red node has a red child
4. every path from root to a leaf contains the same number of black nodes

The key of Okasaki’s insertion is the function `balance` which transforms an unbalanced tree, into a valid red-black tree (as long as a, b, c, and d are valid):

In ML we need GADTs to enforce the invariants.
type αRBtree =
  | Leaf
  | Red( α, RBtree, RBtree)
  | Blk( α, RBtree, RBtree)

let balance =
  function
  | Blk( z , Red( x, a, Red(y,b,c) ) , d )
  | Blk( z , Red( y, Red(x,a,b), c ) , d )
  | Blk( x , a , Red( z, Red(y,b,c), d ) )
  | Blk( x , a , Red( y, b, Red(z,c,d) ) )
    -> Red ( y, Blk(x,a,b), Blk(z,c,d) )
  | x -> x

let insert =
  function ( x , t ) ->
    let ins =
      function
        | Leaf -> Red(x,Leaf,Leaf)
        | c(y,a,b) as z ->
          if x < y then balance c( y, (ins a), b ) else
          if x > y then balance c( y, a, (ins b) ) else z
      in let _(y,a,b) = ins t in Blk(y,a,b)
type αRBtree =
| Leaf
| Red( α , RBtree , RBtree)
| Blk( α , RBtree , RBtree)

let balance =
 function
| Blk( z , Red( x, a, Red(y,b,c) ) , d )
| Blk( z , Red( y, Red(x,a,b), c ) , d )
| Blk( x , a , Red( z, Red(y,b,c), d ) )
| Blk( x , a , Red( y, b, Red(z,c,d) ) )
 -> Red ( y, Blk(x,a,b), Blk(z,c,d) )
| x -> x

let insert =
 function ( x , t ) ->
 let ins =
 function
 | Leaf -> Red(x,Leaf,Leaf)
 | c(y,a,b) as z ->
   if x < y then balance c( y, (ins a), b ) else
   if x > y then balance c( y, a, (ins b) ) else z
 in let _(y,a,b) = ins t in Blk(y,a,b)
type αRBtree =
| Leaf
| Red( α , RBtree , RBtree )
| Blk( α , RBtree , RBtree )

let balance =
function
| Blk( z , Red( x , a , Red(y,b,c) ) , d )
| Blk( z , Red( y , Red(x,a,b) , c ) , d )
| Blk( x , a , Red( z , Red(y,b,c) , d ) )
| Blk( x , a , Red( y , b , Red(z,c,d) ) )
   -> Red( y , Blk(x,a,b), Blk(z,c,d) )
| x -> x

let insert =
function ( x , t ) ->
let ins =
function
| Leaf -> Red(x,Leaf,Leaf)
| c(y,a,b) as z ->
   if x < y then balance c( y , (ins a) , b ) else
   if x > y then balance c( y , a , (ins b) ) else z
in let _(y,a,b) = ins t in Blk(y,a,b)
type \( \alpha \) RBtree =
| Leaf
| Red( \( \alpha \), RBtree, RBtree)
| Blk( \( \alpha \), RBtree, RBtree)

let balance =
function
| Blk( z , Red( x , a , Red(y,b,c) ) , d )
| Blk( z , Red( y , Red(x,a,b), c ) , d )
| Blk( x , a , Red( z , Red(y,b,c), d ) )
| Blk( x , a , Red( y , b , Red(z,c,d) ) )
  -> Red ( y , Blk(x,a,b) , Blk(z,c,d) )
| x -> x

let insert =
function ( x , t ) ->
let ins =
function
| Leaf -> Red(x,Leaf,Leaf)
| c(y,a,b) as z ->
  if x < y then balance c( y , (ins a), b )
  else if x > y then balance c( y , a , (ins b) )
  else z
in let _(y,a,b) = ins t in Blk(y,a,b)
type RBtree = Btree | Rtree
type Rtree = Red(α, Btree, Btree)
type Btree = Blk(α, RBtree, RBtree) | Leaf

type Wrong = Red(α, (Rtree, RBtree) | (RBtree, Rtree))
type Unbal = Blk(α, (Wrong, RBtree) | (RBtree, Wrong))

let balance: (Unbal → Rtree) & ((β\Unbal) → (β\Unbal)) =
  function
  | Blk(z, Red(y, Red(x, a, b), c), d) → Red(y, Blk(x, a, b), Blk(z, c, d))
  | Blk(z, Red(x, a, Red(y, b, c)), d) → Red(y, Blk(x, a, b), Blk(z, c, d))
  | Blk(x, a, Red(z, Red(y, b, c)), d) → Red(y, Blk(x, a, b), Blk(z, c, d))
  | Blk(x, a, Red(y, b, Red(z, c, d))) → Red(y, Blk(x, a, b), Blk(z, c, d))
  | x → x

let insert: (α, Btree) → Btree =
  function (x, t) →
    let ins: (Leaf → Rtree) & (Btree → RBtree\Leaf) & (Rtree → Rtree|Wrong) =
      function
      | Leaf → Red(x, Leaf, Leaf)
      | c(y, a, b) as z →
        if x < y then balance c(y, (ins a), b) else
        if x > y then balance c(y, a, (ins b)) else z
    in let _(y, a, b) = ins t in Blk(y, a, b)
type RBtree = Btree | Rtree

type Rtree = Red(α, Btree , Btree)

type Btree = Blk(α, RBtree, RBtree) | Leaf

type Wrong = Red(α, (Rtree, RBtree) | (RBtree, Rtree))

type Unbal = Blk(α, (Wrong, RBtree) | (RBtree, Wrong))

let balance: (Unbal → Rtree) & ( (β
Unbal) → (β
Unbal)) =

  function
  | Blk( z , Red( y, Red(x,a,b), c ) , d )
  | Blk( z , Red( x, a, Red(y,b,c) ) , d )
  | Blk( x , a , Red( z, Red(y,b,c), d ) )
  | Blk( x , a , Red( y, b, Red(z,c,d) ) )
  | Red ( y, Blk(x,a,b), Blk(z,c,d) )
  | x -> x

let insert: (α, Btree) → Btree =

  function ( x , t ) ->

  let ins: (Leaf → Rtree) & (Btree → RBtree \ Leaf) & (Rtree → Rtree \ Wrong) =

    function
    | Leaf -> Red(x,Leaf,Leaf)
    | c(y,a,b) as z ->
      if x < y then balance c( y, (ins a), b ) else
      if x > y then balance c( y, a, (ins b) ) else z

    in let _(y,a,b) = ins t in Blk(y,a,b)
type RBtree = Btree | Rtree

type Rtree = Red(\(\alpha\), Btree, Btree)

type Btree = Blk(\(\alpha\), RBtree, RBtree) | Leaf

type Wrong = Red(\(\alpha\), (Rtree,RBtree) | (RBtree,Rtree))

type Unbal = Blk(\(\alpha\), (Wrong,RBtree) | (RBtree,Wrong))

let balance: (Unbal \rightarrow Rtree) & ((Unbal \rightarrow Unbal)) =
    function |
      Blk(\(z\), Red(\(y\), Red(x,a,b), c), d)
      Blk(\(z\), Red(x, a, Red(y,b,c)), d)
      Blk(x, a, Red(z, Red(y,b,c), d))
      Blk(x, a, Red(y, b, Red(z,c,d)))
      \rightarrow Red(\(y\), Blk(x,a,b), Blk(z,c,d))
      x \rightarrow x

let insert: (\(\alpha\), Btree) \rightarrow Btree =
    function (x, t) ->
      let ins: (Leaf \rightarrow Rtree) & (Btree \rightarrow RBtree | Leaf) & (Rtree \rightarrow Rtree | Wrong) =
        function |
          Leaf -> Red(x,Leaf,Leaf)
          c(y,a,b) as z ->
            if x < y then balance c(\(y\), (ins a), b) else
            if x > y then balance c(\(y\), a, (ins b)) else z

in
let _(y,a,b) = ins t in Blk(y,a,b)
type RBtree = Btree | Rtree

type Rtree = Red(\(\alpha\), Btree , Btree )

type Btree = Blk(\(\alpha\), RBtree, RBtree) | Leaf

type Wrong = Red(\(\alpha\), (Rtree,RBtree) | (RBtree,Rtree) )

type Unbal = Blk(\(\alpha\), (Wrong,RBtree) | (RBtree,Wrong) )

let balance: (Unbal\(\rightarrow\)Rtree) & ((\(\beta\)\backslash Unbal)\(\rightarrow\)(\(\beta\)\backslash Unbal)) =
  function |
  | Blk( z , Red( y, Red(x,a,b), c ), d )
  | Blk( z , Red( x, a, Red(y,b,c) ) , d )
  | Blk( x , a , Red( z, Red(y,b,c), d ) )
  | Blk( x , a , Red( y, b, Red(z,c,d) ) )
  | -> Red ( y, Blk(x,a,b), Blk(z,c,d) )
  | x -> x

let insert: (\(\alpha\), Btree)\(\rightarrow\)Btree =
  function ( x , t ) ->
  let ins: (Leaf\(\rightarrow\)Rtree) & (Btree\(\rightarrow\)RBtree\(\backslash\)Leaf) & (Rtree\(\rightarrow\)Rtree\(\backslash\)Wrong) =
    function |
    | Leaf -> Red(x,Leaf,Leaf)
    | c(y,a,b) as z ->
    | if x < y then balance c( y, (ins a), b ) else
    | if x > y then balance c( y, a, (ins b) ) else z
    in let _(y,a,b) = ins t in Blk(y,a,b)
type RBtree = Btree | Rtree

type Rtree = Red(α, Btree , Btree )

type Btree = Blk(α, RBtree, RBtree) | Leaf

type Wrong = Red( α, (Rtree,RBtree) | (RBtree,Rtree) )

type Unbal = Blk( α, (Wrong,RBtree) | (RBtree,Wrong) )

let balance: (Unbal → Rtree) & ((β\Unbal) → (β\Unbal)) =

function |
  | Blk(z , Red( y, Red(x,a,b), c ) , d )
  | Blk(z , Red( x, a, Red(y,b,c) ) , d )
  | Blk( x , a , Red( z, Red(y,b,c), d ) )
  | Blk( x , a , Red( y, b, Red(z,c,d) ) )
  | -> Red( y, Blk(x,a,b), Blk(z,c,d) )
  | x -> x

let insert: (α, Btree) → Btree =

function ( x , t ) ->

let ins: (Leaf → Rtree) & (Btree → RBtree\Leaf) & (Rtree → Rtree | Wrong) =

function |
  | Leaf -> Red(x,Leaf,Leaf)
  | c(y,a,b) as z ->
    | if x < y then balance c( y, (ins a), b ) else
    | if x > y then balance c( y, a, (ins b) ) else z
  | in let _(y,a,b) = ins t in Blk(y,a,b)
Type checking the previous definitions is not so difficult. The hard part is to type partial applications:

\[
\text{map} : (\alpha \rightarrow \beta) \rightarrow [\alpha] \rightarrow [\beta]
\]

\[
\text{balance} : (\text{Unbal} \rightarrow \text{Rtree}) \& ((\beta\setminus\text{Unbal}) \rightarrow (\beta\setminus\text{Unbal}))
\]

\[
\text{map balance} : (\text{Unbal} \rightarrow [\text{Rtree}]) \\
\& (\text{Unbal} \rightarrow [\text{Unbal}]) \\
\& ([\alpha\setminus\text{Unbal}] \rightarrow [(\alpha\setminus\text{Unbal})\setminus\text{Rtree}])
\]

Fortunately, programmers (and you) are spared from these gory details.
New languages use union and intersections

Facebook’s Flow:

```javascript
// @flow
function toStringPrimitives(val: number | boolean | string) {
  return String(val);
}

type One = { foo: number };
type Two = { bar: boolean };
type Both = One & Two;

var value: Both = {
  foo: 1,
  bar: true
};
```
New languages use union and intersections

**Typed-Racket**

(let ([a-number 37])
  (if (even? a-number)
      'yes
      'no))
- : Symbol [more precisely: (U 'no 'yes)]
  'no

(: f : (case-> (-> True Integer Integer)
          (-> False Boolean Boolean)))
(define (f condition x)
  (if condition
      (if condition
          (add1 x)
          (not x)))
Typescript
Negation types are proposed in a merge request for TypeScript:

```typescript
function asValid<T extends not null>(value: T, isValid: (value: T) => boolean): T | null {
    return isValid(value) ? value : null;
}
```

declare const x: number;
declare const y: number | null;
asValid(x, n => n >= 0); // OK
asValid(y, n => n >= 0); // Error
Full-fledged connectives for novel type expressivity

The recursive \texttt{flatten} function:

```plaintext
# flatten [ 3 'r' [4 ['true 5'] ] ['false' 'stop'] ] ;
= [ (Bool | 3--5 | 'o'--'u')* ]

\texttt{flatten} \ return \ a \ list \ whose \ element \ type \ is \ the \ union \ of \ the \ types \ of \ all \ the \ leaves:
```
Full-fledged connectives for novel type expressivity

The recursive flatten function:

```
let flatten
 | []  -> []
 | [h ; t] -> (flatten h)@(flatten t)
 | x  -> [x]
```
The recursive `flatten` function:

(* recursive type with union intersection and negation *)

```
type Tree('a) = ('a[An[y*]]) | [(Tree('a))* ]
```

```
let flatten ( (Tree('a)) -> ['a*] )
  | [] -> []
  | [h ; t] -> (flatten h)@(flatten t)
  | x -> [x]
```
Full-fledged connectives for novel type expressivity

The recursive `flatten` function:

(* recursive type with union intersection and negation *)

```ml
type Tree('a) = ('a[|Any*|]) | [ (Tree('a))* ]

let flatten ( (Tree('a)) -> ['a*] )
| [] -> []
| [h ; t] -> (flatten h)@(flatten t)
| x -> [x]
```

The function `flatten` can be applied to any expression since `Tree('a)` unifies with every type. It returns a list whose element type is the union of the types of all the leaves:

```
# flatten [ 3 'r' [4 ['true 5]] [ "quo" [['false] "stop"] ] ];;
- : [ (Bool | 3--5 | 'o'--'u')* ]
  = [ 3 'r' 4 true 5 'quo' false 'stop' ]
```
Encoding of bounded polymorphism

When combined with polymorphic types, set-theoretic types can encode a limited form of bounded polymorphism:

\[ \forall (T_1 \leq \alpha \leq T_2).T \]

is encoded as

\[ T\{\alpha := (\alpha \lor T_1) \land T_2\} \]

For instance:

\[ \text{balance} : (\text{Unbal} \rightarrow \text{Rtree}) \land (\beta \setminus \text{Unbal} \rightarrow \beta \setminus \text{Unbal}) \]

can be read as:

\[ \text{balance} : \forall (\beta \leq \text{not(\text{Unbal})}). (\text{Unbal} \rightarrow \text{Rtree}) \land (\beta \rightarrow \beta) \]

Limited form since you can compare just types with equal bounds
How to understand/explain set-theoretic type connectives?

- The type connectives union, intersection, and negation are completely defined by the subtyping relation:
  - $T_1 \lor T_2$ is the least upper bound of $T_1$ and $T_2$
  - $T_1 \land T_2$ is the greatest lower bound of $T_1$ and $T_2$
  - $\text{not}(T)$ is the only type whose union and intersection with $T$ yield the Any and Empty types, respectively.

- Defining (and deciding) subtyping for type connectives (i.e., $\lor$, $\land$, $\text{not()}$) is far more difficult than for type constructors (i.e., $\rightarrow$, $\times$, $\{\ldots\}$, ...).
  [examples later on]

- Understanding connectives in terms of subtyping is out of reach of simple programmers
The type connectives union, intersection, and negation are completely defined by the subtyping relation:

- $T_1 \lor T_2$ is the least upper bound of $T_1$ and $T_2$
- $T_1 \land T_2$ is the greatest lower bound of $T_1$ and $T_2$
- $\text{not}(T)$ is the only type whose union and intersection with $T$ yield the Any and Empty types, respectively.

Defining (and deciding) subtyping for type connectives (i.e., $\lor$, $\land$, $\text{not}()$) is far more difficult than for type constructors (i.e., $\rightarrow$, $\times$, $\{\ldots\}$, ...).

[examples later on]

Understanding connectives in terms of subtyping is out of reach of simple programmers.

Give a set-theoretic semantics to types
define subtyping semantically
Types as sets of values and semantic subtyping

Each type denotes a set of values:

- **Bool** is the set that contains just two values \{true, false\}.
- **Int** is the set of all the numeric constants: \{0, -1, 1, -2, 2, -3, ...\}.
- **Any** is the set of all values.
- \((T_1, T_2)\) is the set of all the pairs \((v_1, v_2)\) where \(v_1\) is a value in \(T_1\) and \(v_2\) a value in \(T_2\), that is \\{(v_1, v_2) \mid v_1 \in T_1, v_2 \in T_2\}\.
- **\(T_1 \lor T_2\)** is the union of the sets \(T_1\) and \(T_2\), that is \{\(v \mid v \in T_1\) or \(v \in T_2\}\.
- **\(T_1 \land T_2\)** is the intersection of the sets \(T_1\) and \(T_2\), i.e. \{\(v \mid v \in T_1\) and \(v \in T_2\}\.
- **\(\text{not}(T)\)** is the set of all the values not in \(T\), that is \{\(v \mid v \not\in T\}\.
  
  In particular \(\text{not}(\text{Any})\) is the empty set (written Empty).
- **\(T_1 \rightarrow T_2\)** is the set of all function values that when applied to a value in \(T_1\), if they return a value, then this value is in \(T_2\).
Types as sets of values and semantic subtyping

Each type denotes a set of values:

- **Bool** is the set that contains just two values \{true, false\}.
- **Int** is the set of all the numeric constants: \{0, -1, 1, -2, 2, -3, ...\}.
- **Any** is the set of all values.
- \((T_1, T_2)\) is the set of all the pairs \((v_1, v_2)\) where \(v_1\) is a value in \(T_1\) and \(v_2\) a value in \(T_2\), that is \\(\{(v_1, v_2) \mid v_1 \in T_1, v_2 \in T_2\}\).
- \(T_1 \lor T_2\) is the union of the sets \(T_1\) and \(T_2\), that is \(\{v \mid v \in T_1 \text{ or } v \in T_2\}\).
- \(T_1 \land T_2\) is the intersection of the sets \(T_1\) and \(T_2\), i.e. \(\{v \mid v \in T_1 \text{ and } v \in T_2\}\).
- \(\text{not}(T)\) is the set of all the values not in \(T\), that is \(\{v \mid v \not\in T\}\).
  - In particular, \(\text{not}(\text{Any})\) is the empty set (written Empty).
- \(T_1 \rightarrow T_2\) is the set of all function values that when applied to a value in \(T_1\), if they return a value, then this value is in \(T_2\).

Semantic subtyping

Subtyping is set-containment
Semantic Subtyping in a nutshell
Semantic subtyping

\[ t ::= B \mid t \times t \mid t \to t \mid t \lor t \mid t \land t \mid \neg t \mid 0 \mid 1 \]
Semantic subtyping

\[ t ::= B \mid t \times t \mid t \rightarrow t \mid t \lor t \mid t \land t \mid \neg t \mid 0 \mid 1 \]

- **Constructor subtyping** is *easy*: constructors do not mix, *eg.*:

\[
\begin{align*}
  s_2 & \leq s_1 & t_1 & \leq t_2 \\
  s_1 \rightarrow t_1 & \leq s_2 \rightarrow t_2
\end{align*}
\]
Semantic subtyping

\[ t ::= B | \ t \times t | \ t \to t | \ t \lor t | \ t \land t | \neg t | 0 | 1 \]

- **Constructor subtyping** is *easy*:
  constructors do not mix, *eg.*:

  \[
  \begin{align*}
  s_2 &\leq s_1 &\quad t_1 &\leq t_2 \\
  s_1 \to t_1 &\leq s_2 \to t_2 
  \end{align*}
  \]

- **Connective subtyping** is *harder*:
  *connectives* distribute over *constructors*, *eg.*

  \[
  (s_1 \lor s_2) \to t \quad \supsete \quad (s_1 \to t) \land (s_2 \to t)
  \]
Semantic subtyping

$t ::= B \mid t \times t \mid t \rightarrow t \mid t \lor t \mid t \land t \mid \neg t \mid 0 \mid 1$

- Constructor subtyping is *easy*: constructors do not mix, *eg.*:

\[
\begin{align*}
    s_2 \leq s_1 & \quad t_1 \leq t_2 \\
    s_1 \rightarrow t_1 & \leq s_2 \rightarrow t_2
\end{align*}
\]

- Connective subtyping is *harder*: connectives distribute over constructors, *eg.*:

\[
(s_1 \lor s_2) \rightarrow t \quad \supseteq \quad (s_1 \rightarrow t) \land (s_2 \rightarrow t)
\]

Define subtyping semantically: [Hosoya, Pierce]

1. Interpret types as sets (of values)
2. *Define* subtyping as set containment.
First, define an interpretation of types into sets.

\[ \llbracket \rrbracket : \text{Types} \rightarrow \mathcal{P}(\mathcal{D}) \]

such that
First, define an interpretation of types into sets.

\[
[[ \ ]] : \text{Types} \rightarrow \mathcal{P}(\mathcal{D})
\]

such that

- **Connectives** have their set-theoretic interpretation:
  \[
  [[ 0 ]] = \emptyset \quad [[ t_1 \lor t_2 ]] = [[ t_1 ]] \cup [[ t_2 ]]
  
  [[ \lnot t ]] = \mathcal{D} \setminus [[ t ]] \quad [[ t_1 \land t_2 ]] = [[ t_1 ]] \cap [[ t_2 ]]
  \]
First, define an interpretation of types into sets.

\[ [\_]: \text{Types} \rightarrow \mathcal{P}(\mathcal{D}) \]

such that

- **Connectives** have their set-theoretic interpretation:
  \[ [\_] = \emptyset \quad [t_1 \lor t_2] = [t_1] \cup [t_2] \]
  \[ [\neg t] = \mathcal{D} \setminus [t] \quad [t_1 \land t_2] = [t_1] \cap [t_2] \]

- **Constructors** have their natural interpretation:
  \[ [t_1 \times t_2] = [t_1] \times [t_2] \]
  \[ [t_1 \rightarrow t_2] = \{ f \mid f \text{ function from [}t_1\text{] to [}t_2\text{]}\} \]
Semantic subtyping: formalization

First, define an interpretation of types into sets.

\[ [\ ] : \text{Types} \to \mathcal{P}(\mathcal{D}) \]

such that

- **Connectives** have their set-theoretic interpretation:
  \[
  [\emptyset] = \emptyset \\
  [t_1 \lor t_2] = [t_1] \cup [t_2] \\
  [\neg t] = \mathcal{D} \setminus [t] \\
  [t_1 \land t_2] = [t_1] \cap [t_2]
  \]

- **Constructors** have their natural interpretation:
  \[
  [t_1 \times t_2] = [t_1] \times [t_2] \\
  [t_1 \to t_2] = \{ f \mid f \text{ function from } [t_1] \text{ to } [t_2] \}\n  \]

Then define the **subtyping relation** as set-containment.

\[
\text{Then } \textbf{define} \text{ the subtyping relation as set-containment.} \\
\]

\[
s \leq t \iff [s] \subseteq [t]
\]
Semantic subtyping: formalization

First, define an interpretation of types into sets.

\[[\ ]\] : Types → \(\mathcal{P}(\mathcal{D})\)

such that

- **Connectives** have their set-theoretic interpretation:
  \[
  \begin{align*}
  \[[0]\] &= \emptyset \\
  \[[t_1 \lor t_2]\] &= \[[t_1]\] \cup \[[t_2]\] \\
  \[[\neg t]\] &= \mathcal{D} \setminus \[[t]\] \\
  \[[t_1 \land t_2]\] &= \[[t_1]\] \cap \[[t_2]\]
  \end{align*}
  \]

- **Constructors** have their natural interpretation:
  \[
  \begin{align*}
  \[[t_1 \times t_2]\] &= \[[t_1]\] \times \[[t_2]\] \\
  \[[t_1 \to t_2]\] &= \{ f \mid f \text{ function from } \[[t_1]\] \text{ to } \[[t_2]\] \}
  \end{align*}
  \]

Then *define* the subtyping relation as set-containment.

\[ s \leq t \iff \[[s]\] \subseteq \[[t]\] \]

\(\mathcal{D}^2 \subseteq \mathcal{D}\)

\(\mathcal{D}^\mathcal{D} \subseteq \mathcal{D}\)
**Semantic subtyping: formalization**

1. **First**, define an interpretation of types into sets.
   \[ [[ ]] : \text{Types} \rightarrow \mathcal{P}(\mathcal{D}) \]
   such that

   - **Connectives** have their set-theoretic interpretation:
     \[
     [[0]] = \emptyset, \quad [[t_1 \lor t_2]] = [[t_1]] \cup [[t_2]],
     \]
     \[
     [[\neg t]] = \mathcal{D} \setminus [[t]], \quad [[t_1 \land t_2]] = [[t_1]] \cap [[t_2]].
     \]

   - **Constructors** have their natural interpretation:
     \[
     [[t_1 \times t_2]] = [[t_1]] \times [[t_2]],
     \]
     \[
     [[t_1 \rightarrow t_2]] = \{ f \mid f \text{ function from} [[t_1]] \text{ to} [[t_2]] \}\]

   2. **Then define** the subtyping relation as set-containment.
   \[ s \leq t \overset{\text{def}}{\iff} [[s]] \subseteq [[t]] \]
Semantic subtyping: formalization

First, define an interpretation of types into sets.

\[
\llbracket \cdot \rrbracket : \text{Types} \rightarrow \mathcal{P}(D)
\]

such that

- **Connectives** have their set-theoretic interpretation:

  \[
  \llbracket 0 \rrbracket = \emptyset \quad \llbracket t_1 \lor t_2 \rrbracket = \llbracket t_1 \rrbracket \cup \llbracket t_2 \rrbracket \\
  \llbracket \neg t \rrbracket = D \setminus \llbracket t \rrbracket \quad \llbracket t_1 \land t_2 \rrbracket = \llbracket t_1 \rrbracket \cap \llbracket t_2 \rrbracket
  
  \text{cardinality problem}
  
- **Constructors** have their natural interpretation:

  \[
  \llbracket t_1 \times t_2 \rrbracket = \llbracket t_1 \rrbracket \times \llbracket t_2 \rrbracket \\
  \llbracket t_1 \rightarrow t_2 \rrbracket = \{ f \mid f \text{ function from} \llbracket t_1 \rrbracket \text{ to} \llbracket t_2 \rrbracket \}
  
  \mathcal{D}^D \subseteq D
  
Then define the subtyping relation as set-containment.

\[
s \leq t \iff \llbracket s \rrbracket \subseteq \llbracket t \rrbracket
\]

**Key idea**

Do not define what types are
define how they are related
Semantic subtyping: formalization

First, define an interpretation of types into sets.

\[\llbracket\ \rrbracket: \text{Types} \rightarrow \mathcal{P}(\mathcal{D})\]

such that

- **Connectives** have their set-theoretic interpretation:
  \[
  \llbracket 0 \rrbracket = \emptyset \quad \llbracket t_1 \lor t_2 \rrbracket = \llbracket t_1 \rrbracket \cup \llbracket t_2 \rrbracket \\
  \llbracket \neg t \rrbracket = \mathcal{D} \setminus \llbracket t \rrbracket \quad \llbracket t_1 \land t_2 \rrbracket = \llbracket t_1 \rrbracket \cap \llbracket t_2 \rrbracket
  \]

- **Constructors** have their natural interpretation:
  \[
  \llbracket t_1 \times t_2 \rrbracket = \llbracket t_1 \rrbracket \times \llbracket t_2 \rrbracket \\
  \llbracket t_1 \rightarrow t_2 \rrbracket = \{ f \mid f \text{ function from} \llbracket t_1 \rrbracket \text{ to} \llbracket t_2 \rrbracket \}\]

Then define the subtyping relation as set-containment.

\[s \leq t \iff \llbracket s \rrbracket \subseteq \llbracket t \rrbracket\]

**Key idea**

Do not define what types *are* define *how they are related*
Semantic subtyping: formalization

First, define an interpretation of types into sets.

\[ \boxed{} : \text{Types} \to \mathcal{P}(\mathcal{D}) \]

such that

- **Connectives** have their set-theoretic interpretation:
  \[ \boxed{0} = \emptyset \]
  \[ \boxed{t_1 \lor t_2} = \boxed{t_1} \cup \boxed{t_2} \]
  \[ \boxed{\neg t} = \mathcal{D} \setminus \boxed{t} \]
  \[ \boxed{t_1 \land t_2} = \boxed{t_1} \cap \boxed{t_2} \]

- **Constructors** have their natural interpretation:
  \[ \boxed{t_1 \times t_2} = \boxed{t_1} \times \boxed{t_2} \]
  \[ \boxed{t_1 \to t_2} = \{ f \subseteq \mathcal{D}^2 \mid (d_1, d_2) \in f, d_1 \in \boxed{t_1} \Rightarrow d_2 \in \boxed{t_2} \} \]

Then define the subtyping relation as set-containment.

\[ s \leq t \quad \overset{\text{def}}{\iff} \quad \boxed{s} \subseteq \boxed{t} \]

Key idea

Do not define what types *are*
define *how they are related*
Semantic subtyping: formalization

First, define an interpretation of types into sets.

\[ \llbracket \cdot \rrbracket : \text{Types} \rightarrow \mathcal{P}(D) \]

such that

- **Connectives** have their set-theoretic interpretation:
  \[ \llbracket 0 \rrbracket = \emptyset \quad \llbracket t_1 \lor t_2 \rrbracket = \llbracket t_1 \rrbracket \cup \llbracket t_2 \rrbracket \]
  \[ \llbracket \neg t \rrbracket = D \setminus \llbracket t \rrbracket \quad \llbracket t_1 \land t_2 \rrbracket = \llbracket t_1 \rrbracket \cap \llbracket t_2 \rrbracket \]

- ** Constructors** have their natural interpretation:
  \[ \llbracket t_1 \times t_2 \rrbracket = \llbracket t_1 \rrbracket \times \llbracket t_2 \rrbracket \]
  \[ \llbracket t_1 \rightarrow t_2 \rrbracket = \mathcal{P}(\llbracket t_1 \rrbracket \times \llbracket t_2 \rrbracket) \]

Then define the subtyping relation as set-containment.

\[ s \leq t \quad \overset{\text{def}}{\iff} \quad \llbracket s \rrbracket \subseteq \llbracket t \rrbracket \]

**Key idea**

Do not define what types *are* define *how they are related*.

G. Castagna (CNRS)
Semantic subtyping: formalization

First, define an interpretation of types into sets.

\[ \llbracket \cdot \rrbracket : \text{Types} \rightarrow \mathcal{P}(D) \]

such that

- **Connectives** have their set-theoretic interpretation:
  \[ \llbracket 0 \rrbracket = \emptyset \quad \llbracket t_1 \lor t_2 \rrbracket = \llbracket t_1 \rrbracket \cup \llbracket t_2 \rrbracket \]
  \[ \llbracket \neg t \rrbracket = D \setminus \llbracket t \rrbracket \quad \llbracket t_1 \land t_2 \rrbracket = \llbracket t_1 \rrbracket \cap \llbracket t_2 \rrbracket \]

- **Constructors** have their natural interpretation:
  \[ \llbracket t_1 \times t_2 \rrbracket = \llbracket t_1 \rrbracket \times \llbracket t_2 \rrbracket \]
  \[ \llbracket t_1 \rightarrow t_2 \rrbracket = \mathcal{P}(\llbracket t_1 \rrbracket \times \llbracket t_2 \rrbracket) \]

Then **define** the subtyping relation as set-containment.

\[ s \leq t \overset{\text{def}}{\iff} \llbracket s \rrbracket \subseteq \llbracket t \rrbracket \]

**Key idea**

Do not define what types are, define how they are related.
Semantic subtyping: formalization

First, define an interpretation of types into sets.

\[
\llbracket \cdot \rrbracket : \text{Types} \rightarrow \mathcal{P}(\mathcal{D})
\]

such that

- **Connectives** have their set-theoretic interpretation:
  \[
  \llbracket 0 \rrbracket = \emptyset \\
  \llbracket t_1 \lor t_2 \rrbracket = \llbracket t_1 \rrbracket \cup \llbracket t_2 \rrbracket \\
  \llbracket \neg t \rrbracket = \mathcal{D} \setminus \llbracket t \rrbracket \\
  \llbracket t_1 \land t_2 \rrbracket = \llbracket t_1 \rrbracket \cap \llbracket t_2 \rrbracket
  \]

- **Constructors** have the same \( \subseteq \) as their natural interpretation:
  \[
  \llbracket t_1 \times t_2 \rrbracket = \llbracket t_1 \rrbracket \times \llbracket t_2 \rrbracket \\
  \llbracket t_1 \rightarrow t_2 \rrbracket = \mathcal{P}(\llbracket t_1 \rrbracket \times \llbracket t_2 \rrbracket)
  \]

Then **define** the subtyping relation as set-containment.

\[
s \leq t \iff \llbracket s \rrbracket \subseteq \llbracket t \rrbracket
\]

**Key idea**

Do not define what types *are*

define *how they are related*
Semantic subtyping: formalization

- **First**, define an interpretation of types into sets.
  
  \[
  \llbracket \cdot \rrbracket : \text{Types} \rightarrow \mathcal{P}(D)
  \]
  
  such that

  - **Connectives** have their set-theoretic interpretation:
    \[
    \begin{align*}
    \llbracket 0 \rrbracket &= \emptyset \\
    \llbracket t_1 \lor t_2 \rrbracket &= \llbracket t_1 \rrbracket \cup \llbracket t_2 \rrbracket \\
    \llbracket \neg t \rrbracket &= D \setminus \llbracket t \rrbracket \\
    \llbracket t_1 \land t_2 \rrbracket &= \llbracket t_1 \rrbracket \cap \llbracket t_2 \rrbracket
    \end{align*}
    \]

  - **Constructors** have the same \( \subseteq \) as their natural interpretation:
    \[
    \begin{align*}
    \llbracket s_1 \times s_2 \rrbracket \subseteq \llbracket t_1 \times t_2 \rrbracket & \iff \llbracket s_1 \rrbracket \times \llbracket s_2 \rrbracket \subseteq \llbracket t_1 \rrbracket \times \llbracket t_2 \rrbracket \\
    \llbracket s_1 \rightarrow s_2 \rrbracket \subseteq \llbracket t_1 \rightarrow t_2 \rrbracket & \iff \mathcal{P}(\llbracket s_1 \rrbracket \times \llbracket s_2 \rrbracket) \subseteq \mathcal{P}(\llbracket t_1 \rrbracket \times \llbracket t_2 \rrbracket)
    \end{align*}
    \]

- Then **define** the subtyping relation as set-containment.
  
  \[
  s \leq t \defeq \llbracket s \rrbracket \subseteq \llbracket t \rrbracket
  \]

**Key idea**

Do not define what types **are**

**define how they are related**
First, define an interpretation of types into sets.

\[ \llbracket \cdot \rrbracket : \text{Types} \rightarrow \mathcal{P}(\mathcal{D}) \]

such that

- **Connectives** have their set-theoretic interpretation:
  \[ \llbracket 0 \rrbracket = \emptyset \]
  \[ \llbracket t_1 \lor t_2 \rrbracket = \llbracket t_1 \rrbracket \cup \llbracket t_2 \rrbracket \]
  \[ \llbracket \neg t \rrbracket = \mathcal{D} \setminus \llbracket t \rrbracket \]
  \[ \llbracket t_1 \land t_2 \rrbracket = \llbracket t_1 \rrbracket \cap \llbracket t_2 \rrbracket \]

- **Constructors** have the same \( \subseteq \) as their natural interpretation:
  \[ \llbracket s_1 \times s_2 \rrbracket \subseteq \llbracket t_1 \times t_2 \rrbracket \iff \llbracket s_1 \rrbracket \times \llbracket s_2 \rrbracket \subseteq \llbracket t_1 \rrbracket \times \llbracket t_2 \rrbracket \]
  \[ \llbracket s_1 \rightarrow s_2 \rrbracket \subseteq \llbracket t_1 \rightarrow t_2 \rrbracket \iff \mathcal{P}(\llbracket s_1 \rrbracket \times \llbracket s_2 \rrbracket) \subseteq \mathcal{P}(\llbracket t_1 \rrbracket \times \llbracket t_2 \rrbracket) \]

Then define the **subtyping relation** as set-containment.

\[ s \leq t \iff \llbracket s \rrbracket \subseteq \llbracket t \rrbracket \]

**Semantic subtyping**

1. Gives an interpretation satisfying the above constraints;  
2. Gives an algorithm to decide the induced subtyping relation.
1: An interpretation that satisfies the previous constraints.
Looking for $\mathcal{D}$ and $[] : \textbf{Types} \rightarrow \mathcal{P}(\mathcal{D})$ such that:

$$\left[ s_1 \rightarrow s_2 \right] \subseteq \left[ t_1 \rightarrow t_2 \right] \iff \mathcal{P} \left( \left[ s_1 \right] \times \left[ s_2 \right] \right) \subseteq \mathcal{P} \left( \left[ t_1 \right] \times \left[ t_2 \right] \right)$$
1: An interpretation that satisfies the previous constraints.

Looking for $\mathcal{D}$ and $\llbracket \llbracket \rrbracket : \text{Types} \rightarrow \mathcal{P}(\mathcal{D})$ such that:

$$\llbracket s_1 \rightarrow s_2 \rrbracket \subseteq \llbracket t_1 \rightarrow t_2 \rrbracket \iff \mathcal{P}(\llbracket s_1 \rrbracket \times \llbracket s_2 \rrbracket) \subseteq \mathcal{P}(\llbracket t_1 \rrbracket \times \llbracket t_2 \rrbracket)$$

1. $\mathcal{D}$ least solution of $X = X^2 + \mathcal{P}_f(X^2)$
An interpretation that satisfies the previous constraints.

Looking for \( \mathcal{D} \) and \( [\ ] : \text{Types} \to \mathcal{P}(\mathcal{D}) \) such that:

\[
[s_1 \to s_2] \subseteq [t_1 \to t_2] \iff \mathcal{P}([s_1] \times [s_2]) \subseteq \mathcal{P}([t_1] \times [t_2])
\]

\( \mathcal{D} \) least solution of \( X = X^2 + \mathcal{P}_t(X^2) \)
1: An interpretation that satisfies the previous constraints.

Looking for \( \mathcal{D} \) and \( \llbracket \cdot \rrbracket : \text{Types} \rightarrow \mathcal{P}(\mathcal{D}) \) such that:

\[
\llbracket s_1 \rightarrow s_2 \rrbracket \subseteq \llbracket t_1 \rightarrow t_2 \rrbracket \iff \mathcal{P}(\llbracket s_1 \rrbracket \times \llbracket s_2 \rrbracket) \subseteq \mathcal{P}(\llbracket t_1 \rrbracket \times \llbracket t_2 \rrbracket)
\]

1. \( \mathcal{D} \) least solution of \( X = X^2 + \mathcal{P}_f(X^2) \)

2. \( \llbracket \cdot \rrbracket_\mathcal{D} \) is defined as:
1: An interpretation that satisfies the previous constraints.

Looking for \( \mathcal{D} \) and \( [\_] : \text{Types} \rightarrow \mathcal{P}(\mathcal{D}) \) such that:

\[
[\text{s}_1 \rightarrow \text{s}_2] \subseteq [\text{t}_1 \rightarrow \text{t}_2] \iff \mathcal{P}([\text{s}_1] \times [\text{s}_2]) \subseteq \mathcal{P}([\text{t}_1] \times [\text{t}_2])
\]

1. \( \mathcal{D} \) least solution of \( X = X^2 + \mathcal{P}_t(X^2) \)

2. \( [\_]_\mathcal{D} \) is defined as:

- \( [0]_\mathcal{D} = \emptyset \)
- \( [1]_\mathcal{D} = \mathcal{D} \)
- \( [\neg t]_\mathcal{D} = \mathcal{D} \setminus [t]_\mathcal{D} \)
- \( [s \lor t]_\mathcal{D} = [s]_\mathcal{D} \cup [t]_\mathcal{D} \)
- \( [s \land t]_\mathcal{D} = [s]_\mathcal{D} \cap [t]_\mathcal{D} \)
Looking for $\mathcal{D}$ and $[] : \text{Types} \rightarrow \mathcal{P}(\mathcal{D})$ such that:

$$[[s_1 \rightarrow s_2]] \subseteq [[t_1 \rightarrow t_2]] \iff \mathcal{P}([[s_1]] \times [[s_2]]) \subseteq \mathcal{P}([[t_1]] \times [[t_2]])$$

1. $\mathcal{D}$ least solution of $X = X^2 + \mathcal{P}_f(X^2)$

2. $[]_{\mathcal{D}}$ is defined as:

   $[[0]]_{\mathcal{D}} = \emptyset$
   $[[1]]_{\mathcal{D}} = \mathcal{D}$
   $[[\neg t]]_{\mathcal{D}} = \mathcal{D} \setminus [[t]]_{\mathcal{D}}$

   $[[s \lor t]]_{\mathcal{D}} = [[s]]_{\mathcal{D}} \cup [[t]]_{\mathcal{D}}$
   $[[s \land t]]_{\mathcal{D}} = [[s]]_{\mathcal{D}} \cap [[t]]_{\mathcal{D}}$

   $[[s \times t]]_{\mathcal{D}} = [[s]]_{\mathcal{D}} \times [[t]]_{\mathcal{D}}$
   $[[t \rightarrow s]]_{\mathcal{D}} = \mathcal{P}_f([[t]]_{\mathcal{D}} \times [[s]]_{\mathcal{D}})$
1: An interpretation that satisfies the previous constraints.

Looking for $\mathcal{D}$ and $[\mathcal{D}] : \text{Types} \rightarrow \mathcal{P}(\mathcal{D})$ such that:

$$[s_1 \rightarrow s_2] \subseteq [t_1 \rightarrow t_2] \iff \mathcal{P}([s_1] \times [s_2]) \subseteq \mathcal{P}([t_1] \times [t_2])$$

1. $\mathcal{D}$ least solution of $X = X^2 + \mathcal{P}_f(X^2)$

2. $[\mathcal{D}]$ is defined as:

$$[0]_\mathcal{D} = \emptyset \quad [1]_\mathcal{D} = \mathcal{D} \quad [\neg t]_\mathcal{D} = \mathcal{D} \setminus [t]_\mathcal{D}$$

$$[s \lor t]_\mathcal{D} = [s]_\mathcal{D} \cup [t]_\mathcal{D} \quad [s \land t]_\mathcal{D} = [s]_\mathcal{D} \cap [t]_\mathcal{D}$$

$$[s \times t]_\mathcal{D} = [s]_\mathcal{D} \times [t]_\mathcal{D}$$

$$[t \rightarrow s]_\mathcal{D} = \mathcal{P}_f([t]_\mathcal{D} \times [s]_\mathcal{D})$$
An interpretation that satisfies the previous constraints.

Looking for $\mathcal{D}$ and $\llbracket \cdot \rrbracket : \text{Types} \rightarrow \mathcal{P}(\mathcal{D})$ such that:

$$\llbracket s_1 \rightarrow s_2 \rrbracket \subseteq \llbracket t_1 \rightarrow t_2 \rrbracket \iff \mathcal{P}(\llbracket s_1 \rrbracket \times \llbracket s_2 \rrbracket) \subseteq \mathcal{P}(\llbracket t_1 \rrbracket \times \llbracket t_2 \rrbracket)$$

1. $\mathcal{D}$ least solution of $X = X^2 + \mathcal{P}_f(X^2)$

2. $\llbracket \cdot \rrbracket_\mathcal{D}$ is defined as:

$$\llbracket 0 \rrbracket_\mathcal{D} = \emptyset \quad \llbracket 1 \rrbracket_\mathcal{D} = \mathcal{D} \quad \llbracket \neg t \rrbracket_\mathcal{D} = \mathcal{D} \setminus \llbracket t \rrbracket_\mathcal{D}$$

$$\llbracket s \lor t \rrbracket_\mathcal{D} = \llbracket s \rrbracket_\mathcal{D} \cup \llbracket t \rrbracket_\mathcal{D} \quad \llbracket s \land t \rrbracket_\mathcal{D} = \llbracket s \rrbracket_\mathcal{D} \cap \llbracket t \rrbracket_\mathcal{D}$$

$$\llbracket s \times t \rrbracket_\mathcal{D} = \llbracket s \rrbracket_\mathcal{D} \times \llbracket t \rrbracket_\mathcal{D} \quad \llbracket t \rightarrow s \rrbracket_\mathcal{D} = \mathcal{P}_f(\llbracket t \rrbracket_\mathcal{D} \times \llbracket s \rrbracket_\mathcal{D})$$

It is a model:

$$\mathcal{P}_f(X) \subseteq \mathcal{P}_f(Y) \iff X \subseteq Y \iff \mathcal{P}(X) \subseteq \mathcal{P}(Y)$$
An interpretation that satisfies the previous constraints.

Looking for $\mathcal{D}$ and $\llbracket \ ] : \text{Types} \rightarrow \mathcal{P}(\mathcal{D})$ such that:

$$\llbracket s_1 \rightarrow s_2 \rrbracket \subseteq \llbracket t_1 \rightarrow t_2 \rrbracket \iff \mathcal{P}(\llbracket s_1 \rrbracket \times \llbracket s_2 \rrbracket) \subseteq \mathcal{P}(\llbracket t_1 \rrbracket \times \llbracket t_2 \rrbracket)$$

1. $\mathcal{D}$ least solution of $X = X^2 + \mathcal{P}f(X^2)$

2. $\llbracket ] \rrbracket$ is defined as:

$$\llbracket 0 \rrbracket = \emptyset \quad \llbracket 1 \rrbracket = \mathcal{D} \quad \llbracket \neg t \rrbracket = \mathcal{D} \setminus \llbracket t \rrbracket$$
$$\llbracket s \lor t \rrbracket = \llbracket s \rrbracket \cup \llbracket t \rrbracket \quad \llbracket s \land t \rrbracket = \llbracket s \rrbracket \cap \llbracket t \rrbracket$$
$$\llbracket s \times t \rrbracket = \llbracket s \rrbracket \times \llbracket t \rrbracket \quad \llbracket t \rightarrow s \rrbracket = \mathcal{P}(\llbracket t \rrbracket \times \llbracket s \rrbracket)$$

It is a model:

$$\mathcal{P}f(X) \subseteq \mathcal{P}f(Y) \iff X \subseteq Y \iff \mathcal{P}(X) \subseteq \mathcal{P}(Y)$$

It is the best model: for any other model $\llbracket ] \rrbracket$

$$t_1 \leq_{\mathcal{D}'} t_2 \quad \Rightarrow \quad t_1 \leq_{\mathcal{D}} t_2$$
2: An algorithm to decide $t_1 \leq t_2$.

**Step 1:** *Transform the subtyping problem into an emptiness decision problem:*

$$t_1 \leq t_2 \iff [t_1] \subseteq [t_2] \iff [t_1 \land \neg t_2] = \emptyset \iff t_1 \land \neg t_2 \leq 0$$
2: An algorithm to decide $t_1 \leq t_2$.

**Step 1:** Transform the subtyping problem into an emptiness decision problem:

$$ t_1 \leq t_2 \iff [[t_1]] \subseteq [[t_2]] \iff [[t_1 \land \neg t_2]] = \emptyset \iff t_1 \land \neg t_2 \leq 0 $$

**Step 2:** Put the type whose emptiness is to be decided in disjunctive normal form.

$$ \bigvee \bigwedge_{i \in I} \bigwedge_{j \in J} \ell_{ij} $$

where $a ::= b \mid t \times t \mid t \to t \mid 0 \mid 1$ and $\ell ::= a \mid \neg a$
2: An algorithm to decide $t_1 \leq t_2$.

**Step 1:** Transform the subtyping problem into an emptiness decision problem:

$$t_1 \leq t_2 \iff [[t_1]] \subseteq [[t_2]] \iff [[t_1 \land \lnot t_2]] = \emptyset \iff t_1 \land \lnot t_2 \leq 0$$

**Step 2:** Put the type whose emptiness is to be decided in disjunctive normal form.

$$\bigvee_{i \in I} \bigwedge_{j \in J} \ell_{ij}$$

where $a ::= b \mid t \times t \mid t \rightarrow t \mid 0 \mid 1$ and $\ell ::= a \mid \lnot a$

**Step 3:** Simplify mixed intersections:

Mixed summands of the union can be simplified. For instance:

- $(t_1 \times t_2) \land (t_1 \rightarrow t_2) \leq 0$ is always true
- $(t_1 \times t_2) \land \lnot (t_1 \rightarrow t_2) \leq 0$ holds iff $t_1 \times t_2 \leq 0$.  

G. Castagna (CNRS) Four Forms of Polymorphism 113/192
2: An algorithm to decide $t_1 \leq t_2$.

**Step 1:** *Transform the subtyping problem into an emptiness decision problem:*

$$t_1 \leq t_2 \iff \llbracket t_1 \rrbracket \subseteq \llbracket t_2 \rrbracket \iff \llbracket t_1 \land \neg t_2 \rrbracket = \emptyset \iff t_1 \land \neg t_2 \leq 0$$

**Step 2:** *Put the type whose emptiness is to be decided in disjunctive normal form.*

$$\bigvee \bigwedge \ell_{ij} \quad i \in I \: j \in J$$

where $a ::= b \mid t \times t \mid t \to t \mid 0 \mid 1$ and $\ell ::= a \mid \neg a$

**Step 3:** *Simplify mixed intersections:*

Mixed summands of the union can be simplified. For instance:

- $(t_1 \times t_2) \land (t_1 \to t_2) \leq 0$ is always true
- $(t_1 \times t_2) \land \neg (t_1 \to t_2) \leq 0$ holds iff $t_1 \times t_2 \leq 0$.

The problem is reduced to deciding:

$$\bigwedge_{i \in I} s_i \times t_i \bigwedge_{j \in J} \neg (s_j \times t_j) \leq 0 \quad \text{and} \quad \bigwedge_{i \in I} s_i \to t_i \bigwedge_{j \in J} \neg (s_j \to t_j) \leq 0$$

(similarly for basic types)
Step 4: Use the set-theoretic interpretation to simplify the intersections:

Decomposition law for products:

\[ \bigwedge_{i \in I} t_i \times s_i \leq \bigvee_{i \in J} t_i \times s_i \iff \forall J' \subset J. \left( \bigwedge_{i \in I} t_i \leq \bigvee_{i \in J'} t_i \right) \text{ or } \left( \bigwedge_{i \in I} s_i \leq \bigvee_{i \in J \setminus J'} s_i \right) \]

Decomposition law for arrows:

\[ \bigwedge_{i \in I} t_i \rightarrow s_i \leq \bigvee_{i \in J} t_i \rightarrow s_i \iff \exists j \in J. \forall \ I' \subset I. \left( t_j \leq \bigvee_{i \in I'} t_i \right) \text{ or } \left( I' \neq I \text{ et } \bigwedge_{i \in I \setminus I'} s_i \leq s_j \right) \]

Step 5: Memoize (for recursive types) and recurse.
Application to a language.
Language

Syntax

**Exprs**

\[ e ::= x \quad \text{variables} \]

\[ \lambda^{\wedge_{i \in I}s_{i} \rightarrow t_{i}}x.e \quad \text{abstractions} \]

\[ ee \quad \text{applications} \]

\[ (e, e) \quad \text{pairs} \]

\[ \pi_{i}e \quad \text{projections, } i = 1, 2 \]

\[ (x = e \in t)?e:e \quad \text{binding type case} \]

**Values**

\[ v ::= (v, v) \]

\[ \lambda^{\wedge_{i \in I}s_{i} \rightarrow t_{i}}x.e \]
**Syntax**

**Exprs**
\[
\begin{align*}
e & ::= x & \text{variables} \\
   & | \lambda_{i \in I} s_i \rightarrow t_i \ x. e & \text{abstractions} \\
   & | ee & \text{applications} \\
   & | (e, e) & \text{pairs} \\
   & | \pi_i e & \text{projections, } i = 1, 2 \\
   & | (x = e : t) ? e : e & \text{binding type case}
\end{align*}
\]

**Values**
\[
\begin{align*}
v & ::= (v, v) \\
   & | \lambda_{i \in I} s_i \rightarrow t_i \ x. e
\end{align*}
\]

**Semantics**
\[
\begin{align*}
(\lambda_{i \in I} s_i \rightarrow t_i \ x. e) v & \rightarrow e[v/x] \\
\pi_i (v_1, v_2) & \rightarrow v_i & i = 1, 2 \\
(x = v : t) ? e_1 : e_2 & \rightarrow e_1[v/x] & v \in t \\
(x = v : t) ? e_1 : e_2 & \rightarrow e_2[v/x] & v \notin t
\end{align*}
\]
Typing

\[
\begin{array}{c}
\text{[\textsc{Subsumption}]}
\hline
\Gamma \vdash e : t \quad t \leq t' \\
\hline
\Gamma \vdash e : t'
\end{array}
\]
Typing

\[
\begin{align*}
\text{[Subsumption]} & \quad \frac{\Gamma \vdash e : t \quad t \leq t'}{\Gamma \vdash e : t'} \\
\text{[APP]} & \quad \frac{\Gamma \vdash e_1 : t_1 \rightarrow t_2 \quad \Gamma \vdash e_2 : t_1}{\Gamma \vdash e_1 e_2 : t_2} \\
\text{[ABS]} & \quad \frac{\forall i \in I \quad \Gamma, x : s_i \vdash e : t_i}{\Gamma \vdash \lambda^\Lambda_{i \in I} s_i \rightarrow t_i \, x. e : \Lambda_{i \in I} s_i \rightarrow t_i}
\end{align*}
\]
Typing

\[
\begin{align*}
\text{[Subsumption]} & \quad \frac{\Gamma \vdash e : t \quad t \leq t'}{\Gamma \vdash e : t'}
\end{align*}
\]

\[
\begin{align*}
\text{[App]} & \quad \frac{\Gamma \vdash e_1 : t_1 \rightarrow t_2 \quad \Gamma \vdash e_2 : t_1}{\Gamma \vdash e_1 e_2 : t_2}
\end{align*}
\]

\[
\begin{align*}
\text{[Abs]} & \quad \frac{\forall i \in I \quad \Gamma, x : s_i \vdash e : t_i}{\Gamma \vdash \lambda \wedge_{i \in I} s_i \rightarrow t_i x. e : \wedge_{i \in I} s_i \rightarrow t_i}
\end{align*}
\]
Typing

\[
\begin{align*}
\text{[SUBSUMPTION]} & \quad \frac{\Gamma \vdash e : t \quad t \leq t'}{\Gamma \vdash e : t'} \\
\text{[APP]} & \quad \frac{\Gamma \vdash e_1 : t_1 \to t_2 \quad \Gamma \vdash e_2 : t_1}{\Gamma \vdash e_1 e_2 : t_2} \\
\text{[ABS]} & \quad \frac{\forall i \in I \quad \Gamma, x : s_i \vdash e : t_i}{\Gamma \vdash \lambda^{\wedge_{i \in I} s_i \to t_i} x. e : \wedge_{i \in I} s_i \to t_i} \\
\text{[SEL]} & \quad \frac{\Gamma \vdash e : (t_1, t_2)}{\Gamma \vdash \pi_i e : t_i} \\
\text{[PAIR]} & \quad \frac{\Gamma \vdash e_1 : t_1 \quad \Gamma \vdash e_2 : t_2}{\Gamma \vdash (e_1, e_2) : t_1 \times t_2}
\end{align*}
\]
Typing

[SUBSUMPTION]  \[
\frac{\Gamma \vdash e : t \quad t \leq t'}{
\Gamma \vdash e : t'}
\]

[APP]  \[
\frac{\Gamma \vdash e_1 : t_1 \to t_2 \quad \Gamma \vdash e_2 : t_1}{
\Gamma \vdash e_1 e_2 : t_2}
\]

[ABS]  \[
\frac{\forall i \in I \quad \Gamma, x : s_i \vdash e : t_i}{
\Gamma \vdash \lambda \land_{i \in I} s_i \to t_i \cdot e : \land_{i \in I} s_i \to t_i}
\]

[SEL]  \[
\frac{\Gamma \vdash e : (t_1 , t_2)}{
\Gamma \vdash \pi_i e : t_i}
\]

[PAIR]  \[
\frac{\Gamma \vdash e_1 : t_1 \quad \Gamma \vdash e_2 : t_2}{
\Gamma \vdash (e_1, e_2) : t_1 \times t_2}
\]

[TYPECASE]  \[
\frac{\Gamma \vdash e : t_0 \quad \Gamma, x : s_1 \vdash e_1 : t_1 \quad \Gamma, x : s_2 \vdash e_2 : t_2}{
\Gamma \vdash (x = e \in t) ? e_1 : e_2 : \bigvee_{\{i \mid s_i \neq 0\}} t_i}
\]

\[s_1 \equiv t_0 \land t \quad s_2 \equiv t_0 \land \neg t\]
Typing

\[ \Gamma \vdash e : t \quad t \leq t' \quad \Rightarrow \quad \Gamma \vdash e : t' \]

\[ \frac{ \Gamma \vdash e_1 : t_1 \to t_2 \quad \Gamma \vdash e_2 : t_1 }{ \Gamma \vdash e_1 e_2 : t_2 } \]  
\text{[APP]}

\[ \frac{ \Gamma \vdash e_1 : (t_1, t_2) }{ \Gamma \vdash \pi_i e : t_i } \]  
\text{[SEL]}

\[ \frac{ \Gamma \vdash e_1 : t_1 \quad \Gamma \vdash e_2 : t_2 }{ \Gamma \vdash (e_1, e_2) : t_1 \times t_2 } \]  
\text{[PAIR]}

\[ \frac{ \Gamma \vdash e : t_0 \quad \Gamma, x : s_1 \vdash e_1 : t_1 \quad \Gamma, x : s_2 \vdash e_2 : t_2 }{ \Gamma \vdash (x = e \in t)?e_1 : e_2 : \bigvee_{i\mid s_i \neq 0} t_i } \]  
\text{[TYPECASE]}

\[ \forall i \in I \quad \Gamma, x : s_i \vdash e : t_i \quad \Rightarrow \quad \Gamma \vdash \lambda^{\land_{i \in I} s_i \to t_i} x.e : \land_{i \in I} s_i \to t_i \]  
\text{[ABS]}

\[ \text{[SUBSUMPTION]} \]
Typing

\[\Gamma \vdash e : t \quad t \leq t' \quad \vdash e : t'\]

[SUBSUMPTION]

\[\Gamma \vdash e_1 : t_1 \rightarrow t_2 \quad \Gamma \vdash e_2 : t_1 \quad \vdash e_1 e_2 : t_2\]

[APP]

\[\forall i \in I \quad \Gamma, x : s_i \vdash e : t_i \quad \vdash \lambda^{\wedge i \in I s_i \rightarrow t_i} x.e : \bigwedge_{i \in I} s_i \rightarrow t_i\]

[ABS]

\[\Gamma \vdash e : (t_1, t_2) \quad \vdash \pi_i e : t_i\]

[SEL]

\[\Gamma \vdash e_1 : t_1 \quad \Gamma \vdash e_2 : t_2 \quad \vdash (e_1, e_2) : t_1 \times t_2\]

[PAIR]

\[\Gamma \vdash e_1 : t_0 \quad \Gamma, x : s_1 \vdash e_1 : t_1 \quad \Gamma, x : s_2 \vdash e_2 : t_2 \quad \vdash (x = e \in t)?e_1 : e_2 : \bigvee_{\{i | s_i \neq \emptyset\}} t_i \quad s_1 \equiv t_0 \land t \quad s_2 \equiv t_0 \land \neg t\]

[TYPECASE]

A form of occurrence typing
Typing

\[ \text{SUBSUMPTION} \quad \frac{\Gamma \vdash e : t \quad t \leq t'}{\Gamma \vdash e : t'} \]

\[ \text{APP} \quad \frac{\Gamma \vdash e_1 : t_1 \rightarrow t_2 \quad \Gamma \vdash e_2 : t_1}{\Gamma \vdash e_1 \, e_2 : t_2} \]

\[ \text{ABS} \quad \frac{\forall i \in I \quad \Gamma, x : s_i \vdash e : t_i}{\Gamma \vdash \lambda \left( \land_{i \in I} s_i \rightarrow t_i \right)x. e : \land_{i \in I} s_i \rightarrow t_i} \]

\[ \text{SEL} \quad \frac{\Gamma \vdash e : (t_1, t_2)}{\Gamma \vdash \pi_i e : t_i} \]

\[ \text{PAIR} \quad \frac{\Gamma \vdash e_1 : t_1 \quad \Gamma \vdash e_2 : t_2}{\Gamma \vdash (e_1, e_2) : t_1 \times t_2} \]

\[ \text{TYPECASE} \quad \frac{\Gamma \vdash e : t_0 \quad \Gamma, x : s_1 \vdash e_1 : t_1 \quad \Gamma, x : s_2 \vdash e_2 : t_2}{\Gamma \vdash (x = e \in t) ? e_1 : e_2 : \bigvee_{i \mid s_i \neq 0} t_i} \quad \begin{align*} s_1 & \equiv t_0 \land t \\ s_2 & \equiv t_0 \land \neg t \end{align*} \]
Necessary for typing overloaded functions:

\[ \lambda (\text{Int} \rightarrow \text{Int}) \land (\text{Bool} \rightarrow \text{Bool}) \; x. (y = x \in \text{Int}) ? (y + 1) : \text{not}(y) \]
Typing

\[ \frac{\Gamma \vdash e : t \quad t \leq t'}{\Gamma \vdash e : t'} \]

\[ \text{[SUBSUMPTION]} \]

\[ \frac{\Gamma \vdash e_1 : t_1 \rightarrow t_2 \quad \Gamma \vdash e_2 : t_1}{\Gamma \vdash e_1 e_2 : t_2} \]

\[ \frac{\Gamma \vdash e_1 : t_1 \quad \Gamma \vdash e_2 : t_1}{\Gamma \vdash e_1 e_2 : t_2} \]

\[ \text{[APP]} \]

\[ \frac{\Gamma \vdash e : (t_1, t_2)}{\Gamma \vdash \pi_i e : t_i} \]

\[ \frac{\Gamma \vdash e : (t_1, t_2)}{\Gamma \vdash \pi_i e : t_i} \]

\[ \text{[SEL]} \]

\[ \frac{\Gamma \vdash e : t_0 \quad \Gamma, x : s_1 \vdash e_1 : t_1 \quad \Gamma, x : s_2 \vdash e_2 : t_2}{\Gamma \vdash (x = e \in t) ? e_1 : e_2 : \bigvee \{t_i \mid i \in \{s_i \neq 0\} \}} \]

\[ \text{[TYPECASE]} \]

\[ \frac{\Gamma, x : s_i \vdash e : t_0 \quad \Gamma, x : s_i \vdash e : t_0}{\Gamma \vdash \lambda x : s_i \rightarrow t_i \cdot e : \bigwedge_{i \in I} s_i \rightarrow t_i} \]

\[ \text{[ABS]} \]

\[ \frac{\Gamma \vdash e_1 : t_1 \quad \Gamma \vdash e_2 : t_2}{\Gamma \vdash (e_1, e_2) : t_1 \times t_2} \]

\[ \text{[PAIR]} \]

The type system is sound
function double (x) {
    (typeof(x) === "number") ? 2*x : x.concat(x)
}

Exercise
Use the previous rules to check that (1) is well-typed for:

\[ t = (\text{Int} \lor \text{String}) \rightarrow (\text{Int} \lor \text{String}) \]

\[ t = (\text{Int} \rightarrow \text{Int}) \land (\text{String} \rightarrow \text{String}) \]

where \( \text{String} = \mu X. \{\text{concat}: X \rightarrow X\} \)
function double (x) {
    (typeof(x) === "number") ? 2*x : x.concat(x)
}

\[ \lambda^t x. (y = x \in \text{Int})? (2 \ast y) : (y . \text{concat}(y)) \] (1)
function double (x) {
  (typeof(x) === "number") ? 2*x : x.concat(x)
}

λ^t x. (y = x ∈ Int)?(2 * y):(y.concat(y))  \quad (1)

Exercise

Use the previous rules to check that (1) is well-typed for:

- \( t = (\text{Int} \lor \text{String}) \rightarrow (\text{Int} \lor \text{String}) \)
- \( t = (\text{Int} \rightarrow \text{Int}) \land (\text{String} \rightarrow \text{String}) \)

where \( \text{String} = \mu X. \{\text{concat} : X \rightarrow X\} \)
What about the interpretation of types as set of “values”?

I interpreted types into subsets of $D$ rather than into sets of:

$Values \ v ::= (v, v) \mid \lambda \ i \in I : s \ i \to t$.

Define a new interpretation of types:

$\llbracket t \rrbracket_V = \{ v | \vdash v : t \}$

This induces a new subtyping relation:

$t \leq_V s \iff \llbracket t \rrbracket_V \subset \llbracket s \rrbracket_V$

Actually, it is not a new one ... it is the old one:

Theorem [Frisch, Castagna, Benzaken 2002&2008]

$t \leq_V s \iff t \leq_D s$

where $\leq_D$ is the subtyping via $D$ and used to define $\vdash v : t$. 

G. Castagna (CNRS)
What about the interpretation of types as set of “values”?

I interpreted types into subsets of $\mathcal{D}$ rather than into sets of:

$$\text{Values} \quad \nu \ ::= \ (\nu, \nu) \mid \lambda^{i \in I} s_i \to^t x.e$$

Define a new interpretation of types:

$$\llbracket t \rrbracket_V = \{ \nu \mid \nu : t \}$$

This induces a new subtyping relation:

$$t \leq_V s \iff \llbracket t \rrbracket_V \subset \llbracket s \rrbracket_V$$

Actually, it is not a new one ... it is the old one:

Theorem [Frisch, Castagna, Benzaken 2002&2008]

$$t \leq_V s \iff t \leq_D s$$

where $\leq_D$ is the subtyping via $\mathcal{D}$ and used to define $\nu : t$. 

G. Castagna (CNRS) Four Forms of Polymorphism
What about the interpretation of types as set of “values”?

I interpreted types into subsets of $\mathcal{D}$ rather than into sets of:

Values $\nu ::= (\nu, \nu) \mid \lambda^i s \rightarrow t \; x. e$

Define a new interpretation of types:

$$[[t]]_{\nu} = \{ \nu \mid \vdash \nu : t \}$$
What about the interpretation of types as set of “values”? 
I interpreted types into subsets of $\mathcal{D}$ rather than into sets of:

$$\text{Values} \quad \nu ::= (\nu, \nu) \mid \lambda i \in I : s_i \rightarrow t_i \ x . e$$

Define a new interpretation of types:

$$[t]_{\nu} = \{ \nu \mid \vdash \nu : t \}$$

This induces a new subtyping relation:

$$t \leq_{\nu} s \iff [t]_{\nu} \subset [s]_{\nu}$$
What about the interpretation of types as set of "values"?

I interpreted types into subsets of \( \mathcal{D} \) rather than into sets of:

\[
\text{Values} \quad v ::= (v, v) \mid \lambda^i \in I s_i \rightarrow t_i x.e
\]

Define a new interpretation of types:

\[
\llbracket t \rrbracket_V = \{ v \mid \vdash v : t \}
\]

This induces a new subtyping relation:

\[
t \leq_V s \iff \llbracket t \rrbracket_V \subseteq \llbracket s \rrbracket_V
\]

Actually, it is not a new one ... it is the old one:

**Theorem [Frisch, Castagna, Benzaken 2002&2008]**

\[
t \leq_V s \iff t \leq_D s
\]

where \( \leq_D \) is the subtyping via \( \mathcal{D} \) and used to define \( \vdash v : t \)
Closing the circle

Was then $\mathcal{D}$ really necessary?
Closing the circle

Was then $D$ really necessary?

YES!

$\lambda$-abstractions are values and need (sub)typing to be defined. We are in a circular definition
Was then $\mathcal{D}$ really necessary?

YES!

$\lambda$-abstractions are values and need (sub)typing to be defined.
We are in a circular definition

$$[[t]]_V$$
Was then $D$ really necessary?

YES!

$\lambda$-abstractions are values and need (sub)typing to be defined.

We are in a circular definition

$$
\llbracket t \rrbracket \nu \\
\vdash \nu : t
$$
Closing the circle

Was then $\mathcal{D}$ really necessary?

YES!

$\lambda$-abstractions are values and need (sub)typing to be defined. We are in a circular definition

\[
\begin{align*}
\vdash e : t \\
\vdash v : t \\
\end{align*}
\]

\[
\vdash [t]_\nu
\]
Was then $\mathcal{D}$ really necessary?

YES!

$\lambda$-abstractions are values and need (sub)typing to be defined. We are in a circular definition.
Was then $D$ really necessary?

YES!

$\lambda$-abstractions are values and need (sub)typing to be defined. We are in a circular definition
Was then \( \mathcal{D} \) really necessary?

**YES!**

\( \lambda \)-abstractions are values and need (sub)typing to be defined. We are in a circular definition

\[
\vdash e : t \quad \vdash v : t
\]

\[
t \leq t \quad \llbracket t \rrbracket_v
\]
Closing the circle

Was then $D$ really necessary?

YES!

$\lambda$-abstractions are values and need (sub)typing to be defined. We are in a circular definition

\[
t \leq t \quad \text{and} \quad \llbracket t \rrbracket \nu
\]

\[
\vdash e : t \quad \vdash v : t
\]
Closing the circle

Was then $\mathcal{D}$ really necessary?

YES!

$\lambda$-abstractions are values and need (sub)typing to be defined. We are in a circular definition

$$t \leq t$$

$$\Gamma \vdash e : t \quad \Gamma \vdash v : t$$
Was then $\mathcal{D}$ really necessary?

YES!

$\lambda$-abstractions are values and need (sub)typing to be defined. We are in a circular definition

\[
\begin{align*}
\vdash e : t \quad &\vdash v : t \\
[t] &\leq t \\
\end{align*}
\]
Was then $\mathcal{D}$ really necessary?

YES!

$\lambda$-abstractions are values and need (sub)typing to be defined. We are in a circular definition:

\[ t \leq t \quad \vdash e : t \]
\[ [t]_{\mathcal{D}} \]
\[ [t]_{\mathcal{V}} \]
\[ \vdash v : t \]
Was then $\mathcal{D}$ really necessary?

YES!

$\lambda$-abstractions are values and need (sub)typing to be defined. We are in a circular definition:

\[
\begin{align*}
\vdash e : t & \quad \vdash v : t \\
\uparrow & \quad \uparrow \\
\llbracket e \rrbracket_{\mathcal{V}} & \quad \llbracket v \rrbracket_{\mathcal{V}} \\
\downarrow & \quad \downarrow \\
t \leq t & \quad \llbracket t \rrbracket_{\mathcal{D}}
\end{align*}
\]
Was then $\mathcal{D}$ really necessary?

YES!

$\lambda$-abstractions are values and need (sub)typing to be defined. We are in a circular definition: 

\[
\begin{align*}
\vdash e : t & \quad \vdash v : t \\
\downarrow & \quad \downarrow \\
[t] & \quad [t] \\
\downarrow & \quad \downarrow \\
\leq & \quad \leq \\
t & \quad t \\
\end{align*}
\]

\[\mathcal{D}\]

\[
\begin{align*}
[t] & \quad [t] \\
\downarrow & \quad \downarrow \\
\vdash e : t & \quad \vdash v : t \\
\end{align*}
\]
Was then $\mathcal{D}$ really necessary?

YES!

$\lambda$-abstractions are values and need (sub)typing to be defined. We are in a circular definition.

\[ t \leq t \quad \vdash e : t \quad \vdash v : t \]

\[ [t]_\mathcal{D} \]

\[ [t]_\mathcal{V} \]

\[ \text{???} \]
Was then $\mathcal{D}$ really necessary?

**YES!**

$\lambda$-abstractions are values and need (sub)typing to be defined.

*We are in a circular definition*
Was then $\mathcal{D}$ really necessary?

YES!

$\lambda$-abstractions are values and need (sub)typing to be defined.

We are in a circular definition.

Theorem 5.5 [Frisch, Castagna, Benzaken, JACM 2008]
Outline

10 Set-theoretic types

11 Semantic Subtyping

12 Application to a language.

13 Adding Parametric Polymorphism: the Types

14 Adding Parametric Polymorphism: the Language
**Motivating examples: reminder 1**

The recursive **flatten function**:

```plaintext
(* recursive type with union intersection and negation *)
type Tree(α) = (α\[Any\]) | [(Tree(α))] |

(* recursive flatten written in polymorphic CDuce *)
let flatten ( (Tree(α)) -> [α] ) |
[] -> [] |
[; ] -> (flatten h)@(flatten t) |
x -> [x]
```
Motivating examples: reminder 1

**The recursive flatten function:**

(* recursive type with union intersection and negation *)

\[
\text{type Tree}(\alpha) = (\alpha\setminus[\text{Any}*]) \mid [ (\text{Tree}(\alpha))^{*} ]
\]

(* recursive flatten written in polymorphic CDuce *)

\[
\text{let flatten} \ ( (\text{Tree}(\alpha)) \rightarrow [\alpha^{*}] ) \\
| [] \rightarrow [] \\
| [h ; t] \rightarrow (\text{flatten} \ h)@(\text{flatten} \ t) \\
| x \rightarrow [x]
\]

Rationale

The language does not changes apart from the fact that type variables such as \(\alpha\) may occur in type annotations.

G. Castagna (CNRS)
Motivating examples: reminder 1

The recursive `flatten` function:

(* recursive type with union intersection and negation *)

\[
\text{type Tree}(\alpha) = (\alpha \[\text{Any}\*]) \mid [ (\text{Tree}(\alpha))\* ]
\]

(* recursive flatten written in polymorphic CDuce *)

\[
\text{let flatten} = (\text{Tree}(\alpha) \to [\alpha\*])
\mid [] \to []
\mid [h ; t] \to (\text{flatten } h)@(\text{flatten } t)
\mid x \to [x]
\]

Rationale

The language does not changes apart from the fact that type variables such as \(\alpha\) may occur in type annotations.
Type refinement of balance for red-black trees
Type refinement of \texttt{balance} for red-black trees

\begin{verbatim}
let balance: (Unbal \rightarrow Rtree) \& ((\beta \backslash Unbal) \rightarrow (\beta \backslash Unbal)) =

function
| Blk( z , Red( x, a, Red(y,b,c) ) , d )
| Blk( z , Red( y, Red(x,a,b), c ) , d )
| Blk( x , a , Red( z, Red(y,b,c), d ) )
| Blk( x , a , Red( y, b, Red(z,c,d) ) )
    \rightarrow Red ( y, Blk(x,a,b), Blk(z,c,d) )
| x -> x
\end{verbatim}
Naive solution

\[
t ::= B \mid t \times t \mid t \to t \mid t \lor t \mid t \land t \mid \neg t \mid 0 \mid 1
\]
Idea: Use the previous relation since is defined for "ground types"

Let \( \sigma : \text{Vars} \rightarrow \text{ClosedTypes} \) denote ground substitutions. Define:

\[
s \leq t \quad \text{def} \quad \Leftrightarrow \forall \sigma. [s \sigma] \subseteq [t \sigma]
\]

THIS IS A WRONG WAY: TOO MANY PROBLEMS
Naive solution

$$t ::= B \mid t \times t \mid t \to t \mid t \lor t \mid t \land t \mid \neg t \mid 0 \mid 1 \mid \alpha$$

**Idea:** Use the previous relation since it is defined for “ground types”

Let $$\sigma : \text{Vars} \to \text{ClosedTypes}$$ denote ground substitutions. Define:

$$s \leq t \iff \forall \sigma . s\sigma \leq t\sigma$$
Naive solution

\[ t ::= B \mid t \times t \mid t \rightarrow t \mid t \lor t \mid t \land t \mid \neg t \mid 0 \mid 1 \mid \alpha \]

**Idea:** Use the previous relation since is defined for “ground types”

Let \( \sigma : \text{Vars} \rightarrow \text{ClosedTypes} \) denote ground substitutions. Define:

\[ s \leq t \overset{\text{def}}{\iff} \forall \sigma . \ s \sigma \leq t \sigma \]

or equivalently

\[ s \leq t \overset{\text{def}}{\iff} \forall \sigma . [s \sigma] \subseteq [t \sigma] \]
Naive solution

\[ t ::= B \mid t \times t \mid t \rightarrow t \mid t \lor t \mid t \land t \mid \neg t \mid 0 \mid 1 \mid \alpha \]

**Idea:** Use the previous relation since is defined for “ground types”

Let \( \sigma : \text{Vars} \rightarrow \text{ClosedTypes} \) denote ground substitutions. Define:

\[ s \leq t \overset{\text{def}}{\iff} \forall \sigma. \ s\sigma \leq t\sigma \]

or equivalently

\[ s \leq t \overset{\text{def}}{\iff} \forall \sigma. \ [s\sigma] \subseteq [t\sigma] \]

**THIS IS A WRONG WAY: TOO MANY PROBLEMS**
Problems with the naive solution

1. Haruo Hosoya conjectured that deciding $\forall \sigma. \ s\sigma \leq t\sigma$ is \textit{at least} as hard as solving Diophantine equations.
Problems with the naive solution

1. Haruo Hosoya conjectured that deciding $\forall \sigma. \, s\sigma \leq t\sigma$ is at least as hard as solving Diophantine equations.

2. It breaks parametricity:

Property of indivisible types

If $t$ is an indivisible type, then for all possible interpretations of $\alpha$, $t \leq \alpha$ or $\alpha \prec t$ holds.

If $\alpha \prec t$ then the left element of the union in (2) suffices; if $t \leq \alpha$, then $\alpha = (\alpha \setminus t) \lor \lor t$. Thus $(t \times \alpha) = (t \times (\alpha \setminus t)) \lor \lor (t \times t)$. This union is contained component-wise in the one in (2).
Haruo Hosoya conjectured that deciding $\forall \sigma . s\sigma \leq t\sigma$ is \textit{at least} as hard as solving Diophantine equations.

It \textit{breaks} parametricity:

\[(t \times \alpha) \leq (t \times \neg t) \lor (\alpha \times t)\] (2)
Problems with the naive solution

1. Haruo Hosoya conjectured that deciding $\forall \sigma. \ s \sigma \leq t \sigma$ is at least as hard as solving Diophantine equations.

2. It breaks parametricity:

\[(t \times \alpha) \leq (t \times \neg t) \lor (\alpha \times t)\]  

This inclusion holds if and only if $t$ is an indivisible type (eg., a singleton or a basic type):
Problems with the naive solution

1. Haruo Hosoya conjectured that deciding $\forall \sigma. s \sigma \leq t \sigma$ is at least as hard as solving Diophantine equations.

2. It breaks parametricity:

$$\left( t \times \alpha \right) \leq \left( t \times \neg t \right) \lor (\alpha \times t) \tag{2}$$

This inclusion holds if and only if $t$ is an indivisible type (e.g., a singleton or a basic type):

Property of indivisible types

If $t$ is an indivisible type, then for all possible interpretations of $\alpha$

$$t \leq \alpha \quad \text{or} \quad \alpha \leq \neg t$$

holds.
Problems with the naive solution

1. Haruo Hosoya conjectured that deciding $\forall \sigma. s\sigma \leq t\sigma$ is at least as hard as solving Diophantine equations.

2. It *breaks* parametricity:

$$ (t \times \alpha) \leq (t \times \neg t) \lor (\alpha \times t) \quad (2) $$

This inclusion holds if and only if $t$ is an *indivisible* type (e.g., a singleton or a basic type):

**Property of indivisible types**

If $t$ is an *indivisible type*, then for all possible interpretations of $\alpha$

$$ t \leq \alpha \quad \text{or} \quad \alpha \leq \neg t $$

holds.

- If $\alpha \leq \neg t$ then the left element of the union in (2) suffices;
- If $t \leq \alpha$, then $\alpha = (\alpha \setminus t) \lor t$. Thus $(t \times \alpha) = (t \times (\alpha \setminus t)) \lor (t \times t)$. This union is contained component-wise in the one in (2).
Problems with the naive solution

The fact that

\[(t \times \alpha) \leq (t \times \neg t) \lor (\alpha \times t)\]

holds if and only if \(t\) is *indivisible* is really catastrophic:
Problems with the naive solution

The fact that

\[(t \times \alpha) \leq (t \times \neg t) \lor (\alpha \times t)\]

holds if and only if \(t\) is *indivisible* is really catastrophic:

- Deciding subtyping needs deciding indivisibility ... which is very hard.
Problems with the naive solution

The fact that

\[(t \times \alpha) \leq (t \times \neg t) \lor (\alpha \times t)\]

holds if and only if \(t\) is \textit{indivisible} is really catastrophic:

- Deciding subtyping needs deciding indivisibility ... which is very hard.
- \textbf{This subtyping relation breaks parametricity:}
  by subsumption a function generic in its first argument, becomes generic on its second argument.
Problems with the naive solution

The fact that

\[(t \times \alpha) \leq (t \times \neg t) \lor (\alpha \times t)\]

holds if and only if \( t \) is \textit{indivisible} is really catastrophic:

- Deciding subtyping needs deciding indivisibility ... which is very hard.
- \textbf{This subtyping relation breaks parametricity:}
  
  by subsumption a function generic in its first argument, 
  becomes generic on its second argument.

A semantic solution was deemed unfeasible (even w/o arrows)
Problem eschewed by resorting to syntactic solutions: [Hosoya, Frisch, Castagna: POPL 05], [Vouillon: POPL 06].
Problems with the naive solution

The fact that

\[(t \times \alpha) \leq (t \times \neg t) \lor (\alpha \times t)\]

holds if and only if \(t\) is *indivisible* is really catastrophic:

- Deciding subtyping needs deciding indivisibility ... which is very hard.
- **This subtyping relation breaks parametricity:** by subsumption a function generic in its first argument, becomes generic on its second argument.

A semantic solution was deemed unfeasible (even w/o arrows)

Problem eschewed by resorting to syntactic solutions: [Hosoya, Frisch, Castagna: POPL 05], [Vouillon: POPL 06].
A semantic solution

A faint intuition

The loss of parametricity is only due to the interpretation of indivisible types, all the rest works (more or less) smoothly.
A semantic solution

A faint intuition

The loss of parametricity is only due to the interpretation of indivisible types, all the rest works (more or less) smoothly.

The crux of the problem is that for an indivisible type $i$

$$i \leq \alpha \quad \text{or} \quad \alpha \leq -i$$

validity can stutter from one formula to another, missing in this way the uniformity typical of parametricity.
A semantic solution

A faint intuition

The loss of parametricity is only due to the interpretation of indivisible types, all the rest works (more or less) smoothly.

The crux of the problem is that for an indivisible type $i$

$$i \leq \alpha \quad \text{or} \quad \alpha \leq \neg i$$

validity can stutter from one formula to another, missing in this way the uniformity typical of parametricity.

The leitmotiv of this work

A semantic characterization of models where stuttering is absent, should yield a subtyping relation that is:

1. Semantic
2. Intuitive for the programmer
3. Decidable
A semantic solution

Rough idea

**Make indivisible types “splittable”** so that type variables can range over strict subsets of every type, indivisible types included.

[intuition: interpret all non-empty types into infinite sets]
A semantic solution

Rough idea

Make indivisible types “splittable” so that type variables can range over strict subsets of every type, indivisible types included.

[intuition: interpret all non-empty types into infinite sets]

Since this cannot be done at syntactic level, move to the semantic one and replace ground substitutions by semantic assignments:

$$\eta : \text{Vars} \rightarrow \mathcal{P}(D)$$
A semantic solution

Rough idea

**Make indivisible types “splittable”** so that type variables can range over strict subsets of every type, indivisible types included.

[intuition: interpret all non-empty types into infinite sets]

Since this cannot be done at syntactic level, move to the semantic one and replace ground substitutions by semantic assignments:

\[ \eta : \text{Vars} \rightarrow \mathcal{P}(\mathcal{D}) \]

and now the interpretation function takes an extra parameter

\[ \llbracket \rrbracket : \text{Types} \rightarrow \mathcal{P}(\mathcal{D})^{\text{Vars}} \rightarrow \mathcal{P}(\mathcal{D}) \]
A semantic solution

Rough idea

Make indivisible types "splittable" so that type variables can range over strict subsets of every type, indivisible types included.

[intuition: interpret all non-empty types into infinite sets]

Since this cannot be done at syntactic level, move to the semantic one and replace ground substitutions by semantic assignments:

$$\eta : \text{Vars} \rightarrow \mathcal{P}(\mathcal{D})$$

and now the interpretation function takes an extra parameter

$$\llbracket \llbracket \cdot \rrbracket : \text{Types} \rightarrow \mathcal{P}(\mathcal{D})^{\text{Vars}} \rightarrow \mathcal{P}(\mathcal{D})$$

with

$$\begin{align*}
\llbracket \alpha \rrbracket \eta &= \eta(\alpha) \\
\llbracket t_1 \lor t_2 \rrbracket \eta &= \llbracket t_1 \rrbracket \eta \cup \llbracket t_2 \rrbracket \eta \\
\llbracket t_1 \land t_2 \rrbracket \eta &= \llbracket t_1 \rrbracket \eta \cap \llbracket t_2 \rrbracket \eta \\
\llbracket 0 \rrbracket \eta &= \emptyset \\
\llbracket 1 \rrbracket \eta &= \mathcal{D}
\end{align*}$$
A semantic solution

Rough idea

Make indivisible types “splittable” so that type variables can range over strict subsets of every type, indivisible types included.

[intuition: interpret all non-empty types into infinite sets]

Since this cannot be done at syntactic level, move to the semantic one and replace ground substitutions by semantic assignments:

\[ \eta : \text{Vars} \rightarrow \mathcal{P}(\mathcal{D}) \]

and now the interpretation function takes an extra parameter

\[ \llbracket \ ] : \text{Types} \rightarrow \mathcal{P}(\mathcal{D})^{\text{Vars}} \rightarrow \mathcal{P}(\mathcal{D}) \]

with

\[
\begin{align*}
\llbracket \alpha \rrbracket \eta & = \eta(\alpha) \\
\llbracket t_1 \lor t_2 \rrbracket \eta & = \llbracket t_1 \rrbracket \eta \cup \llbracket t_2 \rrbracket \eta \\
\llbracket t_1 \land t_2 \rrbracket \eta & = \llbracket t_1 \rrbracket \eta \cap \llbracket t_2 \rrbracket \eta \\
\llbracket \emptyset \rrbracket \eta & = \emptyset \\
\llbracket 1 \rrbracket \eta & = \mathcal{D}
\end{align*}
\]

and such that it satisfies:

\[
\llbracket t_1 \rightarrow s_1 \rrbracket \eta \subseteq \llbracket t_2 \rightarrow s_2 \rrbracket \eta \quad \iff \quad \mathcal{P}(\llbracket t_1 \rrbracket \eta \times \llbracket s_1 \rrbracket \eta) \subseteq \mathcal{P}(\llbracket t_2 \rrbracket \eta \times \llbracket s_2 \rrbracket \eta)
\]
In this framework the natural definition of subtyping is

\[ s \leq t \iff \forall \eta. \llbracket s \rrbracket \eta \subseteq \llbracket t \rrbracket \eta \]

It “just” remains to find the uniformity condition to avoid stuttering and recover parametricity.
The magic property: convexity

Consider only models of semantic subtyping in which the following convexity property holds

$$\forall \eta. ([t_1] \eta = \emptyset \text{ or } [t_2] \eta = \emptyset) \iff (\forall \eta. [t_1] \eta = \emptyset) \text{ or } (\forall \eta. [t_2] \eta = \emptyset)$$

It avoids stuttering:

$$\forall \eta. ([t] \land \neg \alpha \land \neg \beta \eta = \emptyset \text{ or } [t] \land \alpha \land \beta \eta = \emptyset)$$

— that is, $t \leq \alpha \beta$ or $\alpha \beta \leq t$ holds if and only if $t$ is empty.

There are natural models: all models that map all non-empty types into infinite sets satisfy it [our initial intuition].

A sound, complete, and terminating decision algorithm: the condition gives us exactly the right conditions needed to reuse the subtyping algorithm devised for ground types.

An intuitive relation: the algorithm returns intuitive results (actually, it helps to better understand twisted examples).
The magic property: \textit{convexity}

Consider \textbf{only} models of semantic subtyping in which the following \textit{convexity} property holds

\[
\forall \eta. ([t_1] \eta = \emptyset \text{ or } [t_2] \eta = \emptyset) \iff (\forall \eta. [t_1] \eta = \emptyset) \text{ or } (\forall \eta. [t_2] \eta = \emptyset)
\]

- It avoids stuttering: \[
\forall \eta. ([t \land \neg \alpha] \eta = \emptyset \text{ or } [t \land \alpha] \eta = \emptyset) \quad \text{— that is,}
\]
  \( (t \leq \alpha \text{ or } \alpha \leq \neg t) \) — holds if and only if \( t \) is empty.
The magic property: **convexity**

Consider **only** models of semantic subtyping in which the following **convexity** property holds

\[ \forall \eta. ([t_1] \eta = \emptyset \text{ or } [t_2] \eta = \emptyset) \iff (\forall \eta. [t_1] \eta = \emptyset) \text{ or } (\forall \eta. [t_2] \eta = \emptyset) \]

- It avoids stuttering: \[ \forall \eta. ([t \land \neg \alpha] \eta = \emptyset \text{ or } [t \land \alpha] \eta = \emptyset) \] —that is, \( (t \leq \alpha \text{ or } \alpha \leq \neg t) \) — holds if and only if \( t \) is empty.

- **There are natural models:** all models that map all non-empty types into infinite sets satisfy it [our initial intuition].
Consider only models of semantic subtyping in which the following convexity property holds

\[ \forall \eta.([t_1] \eta = \emptyset \text{ or } [t_2] \eta = \emptyset) \iff (\forall \eta.[t_1] \eta = \emptyset) \text{ or } (\forall \eta.[t_2] \eta = \emptyset) \]

- It avoids stuttering: \( \forall \eta.([t \land \neg \alpha] \eta = \emptyset \text{ or } [t \land \alpha] \eta = \emptyset) \) —that is, \((t \leq \alpha \text{ or } \alpha \leq \neg t)\) holds if and only if \( t \) is empty.

- There are natural models: all models that map all non-empty types into infinite sets satisfy it [our initial intuition].

- A sound, complete, and terminating decision algorithm: the condition gives us exactly the right conditions needed to reuse the subtyping algorithm devised for ground types.
The magic property: convexity

Consider only models of semantic subtyping in which the following convexity property holds

$$\forall \eta. (\llbracket t_1 \rrbracket \eta = \emptyset \text{ or } \llbracket t_2 \rrbracket \eta = \emptyset) \iff (\forall \eta. \llbracket t_1 \rrbracket \eta = \emptyset) \text{ or } (\forall \eta. \llbracket t_2 \rrbracket \eta = \emptyset)$$

- It avoids stuttering: $\forall \eta. (\llbracket t \land \neg \alpha \rrbracket \eta = \emptyset \text{ or } \llbracket t \land \alpha \rrbracket \eta = \emptyset)$ — that is, $(t \leq \alpha \text{ or } \alpha \leq \neg t)$ — holds if and only if $t$ is empty.

- There are natural models: all models that map all non-empty types into infinite sets satisfy it [our initial intuition].

- A sound, complete, and terminating decision algorithm: the condition gives us exactly the right conditions needed to reuse the subtyping algorithm devised for ground types.

- An intuitive relation: the algorithm returns intuitive results (actually, it helps to better understand twisted examples)
The magic property: **convexity**

Consider only models of semantic subtyping in which the following convexity property holds:

\[ \forall \eta.([t_1]_\eta = \emptyset \text{ or } [t_2]_\eta = \emptyset) \iff (\forall \eta.[t_1]_\eta = \emptyset) \text{ or } (\forall \eta.[t_2]_\eta = \emptyset) \]

- It avoids stuttering: \[ \forall \eta.([t \land \lnot \alpha]_\eta = \emptyset \text{ or } [t \land \alpha]_\eta = \emptyset) \] — that is, \((t \leq \alpha \text{ or } \alpha \leq \lnot t)\) holds if and only if \(t\) is empty.

- There are natural models: all models that map all non-empty types into infinite sets satisfy it [our initial intuition].

- A sound, complete, and terminating decision algorithm: the condition gives us exactly the right conditions needed to reuse the subtyping algorithm devised for ground types.

- An intuitive relation: the algorithm returns intuitive results (actually, it helps to better understand twisted examples)
Examples of subtyping relations
Examples

We can internalize properties such as:

\[(\alpha \rightarrow \gamma) \land (\beta \rightarrow \gamma) \sim \alpha \lor \beta \rightarrow \gamma\]
Examples

We can internalize properties such as:

\[(\alpha \rightarrow \gamma) \land (\beta \rightarrow \gamma) \sim \alpha \lor \beta \rightarrow \gamma\]

or distributivity laws:

\[(\alpha \lor \beta \times \gamma) \sim (\alpha \times \gamma) \lor (\beta \times \gamma)\]
Examples

We can internalize properties such as:

\[(\alpha \to \gamma) \wedge (\beta \to \gamma) \sim \alpha \lor \beta \to \gamma\]

or distributivity laws:

\[(\alpha \lor \beta \times \gamma) \sim (\alpha \times \gamma) \lor (\beta \times \gamma)\]

and combining them deduce:

\[(\alpha \times \gamma \to \delta_1) \wedge (\beta \times \gamma \to \delta_2) \leq (\alpha \lor \beta \times \gamma) \to \delta_1 \lor \delta_2\]
Examples

We can internalize properties such as:

\[(\alpha \rightarrow \gamma) \land (\beta \rightarrow \gamma) \sim \alpha \lor \beta \rightarrow \gamma\]

or distributivity laws:

\[(\alpha \lor \beta \times \gamma) \sim (\alpha \times \gamma) \lor (\beta \times \gamma)\]

and combining them deduce:

\[(\alpha \times \gamma \rightarrow \delta_1) \land (\beta \times \gamma \rightarrow \delta_2) \leq (\alpha \lor \beta \times \gamma) \rightarrow \delta_1 \lor \delta_2\]

Of course the problematic relation never holds, whatever the \( t \):

\[(t \times \alpha) \not\leq (t \times \neg t) \lor (\alpha \times t)\]
We can prove relevant relations on infinite types, *eg.*, for the type of generic $\alpha$-lists:

\[
\alpha\text{-list} = \mu z. (\alpha \times z) \lor \text{nil}
\]
We can prove relevant relations on infinite types, eg., for the type of generic $\alpha$-lists:

$$\alpha\text{-list} = \mu z. (\alpha \times z) \lor \text{nil}$$

we can prove that it contains both the $\alpha$-lists of even length

$$\mu z. (\alpha \times (\alpha \times z)) \lor \text{nil} \leq \mu z. (\alpha \times z) \lor \text{nil}$$

$\alpha$-lists of even length $\alpha$-lists

and the $\alpha$-lists with of odd length

$$\mu z. (\alpha \times (\alpha \times z)) \lor (\alpha \times \text{nil}) \leq \mu z. (\alpha \times z) \lor \text{nil}$$

$\alpha$-lists of odd length $\alpha$-lists
We can prove relevant relations on infinite types, *eg.*, for the type of generic \(\alpha\)-lists:

\[
\alpha\text{-list} = \mu z. (\alpha \times z) \lor \text{nil}
\]

we can prove that it contains both the \(\alpha\)-lists of even length

\[
\mu z. (\alpha \times (\alpha \times z)) \lor \text{nil} \leq \mu z. (\alpha \times z) \lor \text{nil}
\]

and the \(\alpha\)-lists with of odd length

\[
\mu z. (\alpha \times (\alpha \times z)) \lor (\alpha \times \text{nil}) \leq \mu z. (\alpha \times z) \lor \text{nil}
\]

and that it is itself contained in the union of the two, that is:

\[
\alpha\text{-list} \sim (\mu z. (\alpha \times (\alpha \times z)) \lor \text{nil}) \lor (\mu z. (\alpha \times (\alpha \times z)) \lor (\alpha \times \text{nil}))
\]
We can prove relevant relations on infinite types, *eg.*, for the type of generic $\alpha$-lists:

$$\alpha\text{-list} = \mu z.(\alpha \times z) \cup \text{nil}$$

we can prove that it contains both the $\alpha$-lists of even length

$$\mu z.(\alpha \times (\alpha \times z)) \cup \text{nil} \leq \mu z.(\alpha \times z) \cup \text{nil}$$

and the $\alpha$-lists with of odd length

$$\mu z.(\alpha \times (\alpha \times z)) \cup (\alpha \times \text{nil}) \leq \mu z.(\alpha \times z) \cup \text{nil}$$

and that it is itself contained in the union of the two, that is:

$$\alpha\text{-list} \sim (\mu z.(\alpha \times (\alpha \times z)) \cup \text{nil}) \cup (\mu z.(\alpha \times (\alpha \times z)) \cup (\alpha \times \text{nil}))$$

And we can prove far more complicated relations (see paper).
Subtyping algorithm
Subtyping Algorithm: $t_1 \leq t_2$

**Step 1:** *Transform the subtyping problem into an emptiness decision problem:*

$$t_1 \leq t_2 \iff \forall \eta. [[t_1]]\eta \subseteq [[t_2]]\eta \iff \forall \eta. [[t_1 \land \neg t_2]]\eta = \emptyset \iff t_1 \land \neg t_2 \leq 0$$
Subtyping Algorithm: $t_1 \leq t_2$

**Step 1:** Transform the subtyping problem into an emptiness decision problem:

$$t_1 \leq t_2 \iff \forall \eta. [[t_1]]\eta \subseteq [[t_2]]\eta \iff \forall \eta. [[t_1 \land \neg t_2]]\eta = \emptyset \iff t_1 \land \neg t_2 \leq \emptyset$$

**Step 2:** Put the type whose emptiness is to be decided in disjunctive normal form.

$$\bigvee_{i \in I} \bigwedge_{j \in J} \ell_{ij}$$

where $a ::= b \mid t \times t \mid t \rightarrow t \mid 0 \mid 1 \mid \alpha$ and $\ell ::= a \mid \neg a$
Subtyping Algorithm: $t_1 \leq t_2$

**Step 1:** Transform the subtyping problem into an emptiness decision problem:

$$t_1 \leq t_2 \iff \forall \eta. [[t_1]]\eta \subseteq [[t_2]]\eta \iff \forall \eta. [[t_1 \land \neg t_2]]\eta = \emptyset \iff t_1 \land \neg t_2 \leq \emptyset$$

**Step 2:** Put the type whose emptiness is to be decided in disjunctive normal form.

$$\bigvee_{i \in I} \bigwedge_{j \in J} \ell_{ij}$$

where $a ::= b \mid t \times t \mid t \rightarrow t \mid 0 \mid 1 \mid \alpha$ and $\ell ::= a \mid \neg a$

**Step 3:** Simplify mixed intersections:

Solve:

$$\bigwedge_{i \in I} a_i \bigwedge_{j \in J} \neg a'_j \bigwedge_{h \in H} \alpha_h \bigwedge_{k \in K} \neg \beta_k$$

where all $a$ have the same toplevel constructor.
Step 4: **Eliminate toplevel negative variables.**

\[ \forall \eta. [[t]] \eta = \emptyset \iff \forall \eta. [[t[\neg \alpha/\alpha]]] \eta = \emptyset \]

so replace \( \neg \beta_k \) for \( \beta_k \) (for all \( k \in K \))

Solve:

\[ \bigwedge_{i \in I} a_i \bigwedge_{j \in J} \neg a'_j \bigwedge_{h \in H} \alpha_h \]
**Step 4: Eliminate toplevel negative variables.**

\[ \forall \eta. \llbracket t \rrbracket \eta = \emptyset \iff \forall \eta. \llbracket t[\alpha/\alpha] \rrbracket \eta = \emptyset \]

so replace \( -\beta_k \) for \( \beta_k \) (forall \( k \in K \))

Solve:

\[
\bigwedge_{i \in I} a_i \bigwedge_{j \in J} \neg a_j' \bigwedge_{h \in H} \alpha_h
\]

**Step 5: Eliminate toplevel variables.**

\[
\bigwedge_{t_1 \times t_2 \in P} t_1 \times t_2 \bigwedge_{h \in H} \alpha_h \leq \bigvee_{t_1' \times t_2' \in N} t_1' \times t_2'
\]

holds if and only if

\[
\bigwedge_{t_1 \times t_2 \in P} t_1 \sigma \times t_2 \sigma \bigwedge_{h \in H} \gamma^1_h \times \gamma^2_h \leq \bigvee_{t_1' \times t_2' \in N} t_1' \sigma \times t_2' \sigma
\]

where \( \sigma = [(\gamma^1_h \times \gamma^2_h) \lor \alpha_h / \alpha_h]_{h \in H} \) (similarly for arrows)
Step 6: Eliminate toplevel constructors, memoize, and recurse.

\[ \bigwedge_{t_1 \times t_2 \in P} t_1 \times t_2 \leq \bigvee_{t'_1 \times t'_2 \in N} t'_1 \times t'_2 \] (3)

Equation (3) holds if and only if for all \( N' \subseteq N \),

\[
\forall \eta. \left( \left[ \bigwedge_{t_1 \times t_2 \in P} t_1 \land \bigwedge_{t'_1 \times t'_2 \in N'} \neg t'_1 \right]\eta = \emptyset \right) \text{ or } \left( \left[ \bigwedge_{t_1 \times t_2 \in P} t_2 \land \bigwedge_{t'_1 \times t'_2 \in N \setminus N'} \neg t'_2 \right]\eta = \emptyset \right)
\]

Apply \textit{convexity} to distribute the quantification over the or’s:

\[
\forall \eta. \left( \left[ \bigwedge_{t_1 \times t_2 \in P} t_1 \land \bigwedge_{t'_1 \times t'_2 \in N'} \neg t'_1 \right]\eta = \emptyset \right) \text{ or } \forall \eta. \left( \left[ \bigwedge_{t_1 \times t_2 \in P} t_2 \land \bigwedge_{t'_1 \times t'_2 \in N \setminus N'} \neg t'_2 \right]\eta = \emptyset \right)
\]

Yielding the following simplification:

\[
\forall N' \subseteq N. \left( \bigwedge_{t_1 \times t_2 \in P} t_1 \leq \bigvee_{t'_1 \times t'_2 \in N'} t'_1 \right) \text{ or } \left( \bigwedge_{t_1 \times t_2 \in P} t_2 \leq \bigvee_{t'_1 \times t'_2 \in N \setminus N'} t'_2 \right)
\]

(similarly for arrows)
Outline

10 Set-theoretic types

11 Semantic Subtyping

12 Application to a language.

13 Adding Parametric Polymorphism: the Types

14 Adding Parametric Polymorphism: the Language
A motivating example in Haskell

\begin{verbatim}
map :: (\alpha \to \beta) \to [\alpha] \to [\beta]
map f l = case l of
  | [] -> []
  | (x : xs) -> (f x : map f xs)
\end{verbatim}
A motivating example in Haskell

\[ \text{map} :: (\alpha \to \beta) \to [\alpha] \to [\beta] \]

\[
\text{map } f \ l = \text{case } l \ of \\
| [] \to [] \\
| (x : xs) \to (f \ x : \text{map } f \ xs)
\]

\[
\text{even} :: (\text{Int} \to \text{Bool}) \land ((\alpha \setminus \text{Int}) \to (\alpha \setminus \text{Int}))
\]

\[
\text{even } x = \text{case } x \ of \\
| \text{Int} \to (x \mod 2) == 0 \\
| _ \to x
\]
A motivating example in Haskell (almost)  

```haskell
map :: (α → β) → [α] → [β]
map f l = case l of
  | []    -> []
  | (x : xs) -> (f x : map f xs)

even :: (Int → Bool) ∧ ((α\Int) → (α\Int))
even x = case x of
  | Int    -> (x ‘mod’ 2) == 0
  | _      -> x
```
A motivating example in Haskell (almost) [cf. typing of balance]

map :: (\alpha \rightarrow \beta) \rightarrow [\alpha] \rightarrow [\beta]
map f l = case l of
  | [] -> []
  | (x : xs) -> (f x : map f xs)

even :: (Int \rightarrow \text{Bool}) \land ((\alpha \setminus \text{Int}) \rightarrow (\alpha \setminus \text{Int}))
even x = case x of
  | Int -> (x ‘\text{mod}‘ 2) == 0
  | _ -> x

Expression: if the argument is an integer then return the Boolean expression otherwise return the argument
A motivating example in Haskell (almost) [cf. typing of balance]

map :: (α → β) → [α] → [β]
map f l = case l of
    | []    -> []
    | (x : xs) -> (f x : map f xs)

even :: (Int → Bool) ∧ ((α\Int) → (α\Int))
even x = case x of
    | Int    -> (x ‘mod‘ 2) == 0
    | _      -> x

- **Expression**: if the argument is an integer then return the Boolean expression otherwise return the argument
- **Type**: when applied to an Int it returns a Bool; when applied to an argument that is not an Int it returns a result of the same type.
map :: (\alpha \rightarrow \beta) \rightarrow [\alpha] \rightarrow [\beta]
map f l = case l of
    [] -> []
    (x : xs) -> (f x : map f xs)

even :: (Int \rightarrow \text{Bool}) \wedge ((\alpha \setminus \text{Int}) \rightarrow (\alpha \setminus \text{Int}))
even x = case x of
    Int -> (x 'mod' 2) == 0
    _ -> x

- **Expression:** if the argument is an integer then return the Boolean expression otherwise return the argument
- **Type:** when applied to an \texttt{Int} it returns a \texttt{Bool}; when applied to an argument that is not an \texttt{Int} it returns a result \textit{of the same type}. 


A motivating example in Haskell (almost) [cf. typing of balance]

map :: \(\alpha \to \beta\) \to \left[\alpha\right] \to \left[\beta\right]

\[
\text{map } f \text{ } l = \text{case } l \text{ of } \\
| [\ ] \to [\ ] \\
| (x : xs) \to (f \ x : \text{map } f \ xs)
\]

even :: (Int \to \text{Bool}) \land ((\alpha \to \text{Int}) \to (\alpha \to \text{Int}))

even \ x = \text{case } x \text{ of } \\
| \text{Int} \to (x \ 'mod' \ 2 =\ 0) \\
| _ \to x

- **Expression:** if the argument is an integer then return the Boolean expression otherwise return the argument
- **Type:** when applied to an Int it returns a Bool; when applied to an argument that is not an Int it returns a result of the same type.
A motivating example in Haskell (almost) \([\text{cf. typing of balance}]\)

\[
\begin{align*}
\text{map} :: & \quad \alpha \rightarrow \beta \rightarrow \alpha \rightarrow \beta \\
\text{map} f l = & \quad \text{case } l \text{ of} \\
& \quad \begin{cases}
\text{[]} -> \text{[]} \\
(x : xs) -> (f x : \text{map } f \ xs)
\end{cases}
\end{align*}
\]

\[
\begin{align*}
\text{even} :: & \quad (\text{Int} \rightarrow \text{Bool}) \times ((\alpha \text{ Int}) \rightarrow (\alpha \text{ Int})) \\
\text{even} x = & \quad \text{case } x \text{ of} \\
& \quad \begin{cases}
\text{Int} -> (x \ \text{`mod` } 2) == 0 \\
\_ -> x
\end{cases}
\end{align*}
\]

- **Expression:** if the argument is an integer then return the Boolean expression otherwise return the argument
- **Type:** when applied to a \text{Int} it returns a \text{Bool}; when applied to an argument that is not a \text{Int} it returns a result of the same type.
A motivating example in Haskell (almost) [cf. typing of \textit{balance}]

\[
\text{map} :: (\alpha \to \beta) \to [\alpha] \to [\beta]
\]

\[
\text{map } f \ l = \text{case } l \text{ of} \\
\quad \text{| [] } \rightarrow \text{ []} \\
\quad \text{| (x : xs) } \rightarrow \text{ (f x : map f xs)}
\]

\[
\text{even} :: (\text{Int}\to \text{Bool}) \land (\langle \alpha \mid \text{Int} \rangle \to \langle \alpha \mid \text{Int} \rangle)
\]

\[
\text{even } x = \text{case } x \text{ of} \\
\quad \text{| Int } \rightarrow \text{ (x ‘mod‘ 2) == 0} \\
\quad \text{| _ } \rightarrow \text{ x}
\]

- **Expression:** if the argument is an integer then return the Boolean expression otherwise return the argument
- **Type:** when applied to an \textit{Int} it returns a \textit{Bool}; when applied to an argument that is not an \textit{Int} it returns a result \textit{of the same type}.

Common pattern for functional data structures: \textit{red-black trees balancing}; \textit{ZDD operations}; \textit{XML nodes modification}
map :: \((\alpha \rightarrow \beta) \rightarrow [\alpha] \rightarrow [\beta]\)

\[
\text{map } f \ l = \text{case } l \ of \\
\mid \ [] \rightarrow [] \\
\mid (x : xs) \rightarrow (f \ x : \text{map } f \ xs)
\]

even :: \((\text{Int} \rightarrow \text{Bool}) \land ((\alpha \downarrow \text{Int}) \rightarrow (\alpha \downarrow \text{Int}))\)

even x = \text{case } x \ of \\
\mid \text{Int} \rightarrow (x \ 'mod' \ 2) == 0 \\
\mid \_ \rightarrow x

Expression: if the argument is an integer then return the Boolean expression otherwise return the argument

Type: when applied to an \text{Int} it returns a \text{Bool}; when applied to an argument that is not an \text{Int} it returns a result \textit{of the same type}.

The combination of type-case and intersections yields statically typed \textit{dynamic overloading}.
A motivating example in Haskell (almost) [cf. typing of \textit{balance}]

map :: (\alpha \to \beta) \to [\alpha] \to [\beta]
map f l = case l of
  | [] -> []
  | (x : xs) -> (f x : map f xs)

even :: (Int \to \text{Bool}) \wedge ((\alpha \setminus \text{Int}) \to (\alpha \setminus \text{Int}))
even x = case x of
  | Int -> (x `mod` 2) == 0
  | _ -> x

This example as a yardstick. I want to define a language that:

1. Can define both \textit{map} and \textit{even}
A motivating example in Haskell (almost) [cf. typing of balance]

map :: (\alpha \rightarrow \beta) \rightarrow [\alpha] \rightarrow [\beta]
map f l = case l of
    | [] -> []
    | (x : xs) -> (f x : map f xs)

even :: (Int \rightarrow Bool) \wedge ((\alpha \setminus \text{Int}) \rightarrow (\alpha \setminus \text{Int}))
even x = case x of
    | Int -> (x 'mod' 2) == 0
    | _ -> x

This example as a yardstick. I want to define a language that:
1. Can define both map and even
2. Can check the types specified in the signature
A motivating example in Haskell (almost)  

[cf. typing of balance]  

map :: (α → β) → [α] → [β]  
map f l = case l of  
  | [] -> []  
  | (x : xs) -> (f x : map f xs)  

even :: (Int → Bool) ∧ ((α\Int) → (α\Int))  
even x = case x of  
  | Int -> (x ‘mod‘ 2) == 0  
  | _ -> x  

This example as a yardstick. I want to define a language that:  

1. Can define both `map` and `even`  
2. Can *check* the types specified in the signature  
3. Can *deduce* the type of the partial application `map even`
A motivating example in Haskell (almost) [cf. typing of balance]

map :: (α → β) → [α] → [β]
map f l = case l of
  | []   -> []
  | (x : xs) -> (f x : map f xs)

even :: (Int → Bool) ∧ ((α \ Int) → (α \ Int))
even x = case x of
  | Int   -> (x ‘mod‘ 2) == 0
  | _     -> x

This example as a yardstick. I want to define a language that:

1. Can define both map and even
2. Can check the types specified in the signature
3. Can deduce the type of the partial application map even
A motivating example in Haskell (almost) [cf. typing of balance]

map :: (α → β) → [α] → [β]
map f l = case l of
  [] -> []
  (x : xs) -> (f x : map f xs)

even :: (Int → Bool) ∧ ((α \ Int) → (α \ Int))
even x = case x of
  Int -> (x ‘mod‘ 2) == 0
  _ -> x

This example as a yardstick. I want to define a language that:

1. Can define both `map` and `even` [Tough!]
2. Can check the types specified in the signature
3. Can deduce the type of the partial application `map even`
A motivating example in Haskell (almost) [cf. typing of balance]

map :: (α → β) → [α] → [β]
map f l = case l of
  | [] -> []
  | (x : xs) -> (f x : map f xs)

even :: (Int → Bool)∧((α\Int) → (α\Int))
even x = case x of
  | Int -> (x ‘mod‘ 2) == 0
  | _ -> x

We expect \textbf{map even} to have the following type:

\[
([\text{Int}] \rightarrow [\text{Bool}])∧
([α\text{\Int}] \rightarrow [α\text{\Int}])∧
([α\text{\Int}] \rightarrow [(α\text{\Int})∨\text{Bool}])
\]
A motivating example in Haskell (almost)  

\[
\text{map} :: (\alpha \to \beta) \to [\alpha] \to [\beta]
\]
\[
\text{map } f \ l = \text{case } l \text{ of } \\
| \ [] \to [] \\
| (x : xs) \to (f \ x : \text{map } f \ xs)
\]

\[
\text{even} :: (\text{Int} \to \text{Bool}) \land ((\alpha \land \text{Int}) \to (\alpha \land \text{Int}))
\]
\[
\text{even } x = \text{case } x \text{ of } \\
| \ \text{Int} \to (x \mod 2) == 0 \\
| \ _ \to x
\]

We expect \text{map even} to have the following type:

\[
(\text{[Int]} \to \text{[Bool]}) \land \\
(\text{[\alpha \land \text{Int}]} \to \text{[\alpha \land \text{Int}]}) \land \\
(\text{[\alpha \lor \text{Int}]} \to \text{[(\alpha \land \text{Int}) \lor \text{Bool}]})
\]

- int lists are transformed into bool lists
- lists w/o ints return the same type
- ints in the arg. are replaced by bools
A motivating example in Haskell (almost)  [cf. typing of balance]

map :: (α → β) → [α] → [β]
map f l = case l of
    | [] -> []
    | (x : xs) -> (f x : map f xs)

even :: (Int → Bool) ∧ ((α\Int) → (α\Int))
even x = case x of
    | Int -> (x ‘mod‘ 2) == 0
    | _ -> x

We expect \textbf{map even} to have the following type:

\[
([\text{Int}] \rightarrow [\text{Bool}]) \land \\
([α\text{Int}] \rightarrow [α\text{Int}]) \land \\
([α\text{Int}] \rightarrow [(α\text{Int})∪\text{Bool}])
\]

int lists are transformed into bool lists
lists w/o ints return the same type
ints in the arg. are replaced by bools

Difficult because of expansion: needs \textit{a set of type substitutions} —rather than just one— to unify the domain and the argument types.
The rule for applications

1. In the type system:

\[
\begin{align*}
(A_{\text{PPL}}) \\
\Gamma \vdash e_1 : s \rightarrow u & \quad \Gamma \vdash e_2 : s \\
\hline
\Gamma \vdash e_1 e_2 : u \\
\end{align*}
\]

[The type of the function is subsumed to an arrow and the type of the argument is subsumed to the domain of this arrow].
The rule for applications

1. In the type system:

\[
\begin{align*}
(A_{\text{PPL}}) \\
\Gamma \vdash e_1 : s \to u \quad \Gamma \vdash e_2 : s \\
\hline
\Gamma \vdash e_1 e_2 : u
\end{align*}
\]

[The type of the function is subsumed to an arrow and the type of the argument is subsumed to the domain of this arrow].

2. Subsumption elimination:

\[
\begin{align*}
(A_{\text{PPL-ALGORITHM}}) \\
\Gamma \vdash_{\mathcal{A}} e_1 : t \quad \Gamma \vdash_{\mathcal{A}} e_2 : s \\
\hline
\Gamma \vdash_{\mathcal{A}} e_1 e_2 : \min\{u \mid t \leq s \to u\} \\
\end{align*}
\]

\[
\begin{align*}
t \leq 0 \to 1 \\
s \leq \text{dom}(t)
\end{align*}
\]
The rule for applications

1. In the type system:

\[ \begin{align*}
(\text{APPL}) \\
\Gamma \vdash e_1 : s \rightarrow u & \quad \Gamma \vdash e_2 : s \\
\hline \\
\Gamma \vdash e_1 e_2 : u 
\end{align*} \]

[The type of the function is subsumed to an arrow and the type of the argument is subsumed to the domain of this arrow].

2. Subsumption elimination:

\[ \begin{align*}
(\text{APPL-ALGORITHM}) \\
\Gamma \vdash \mathcal{A} e_1 : t & \quad \Gamma \vdash \mathcal{A} e_2 : s \\
\hline \\
\Gamma \vdash \mathcal{A} e_1 e_2 : \min\{u \mid t \leq s \rightarrow u\} 
\end{align*} \]

\[ t \leq 0 \rightarrow 1 \]
\[ s \leq \text{dom}(t) \]

[Conditions for typeability]
The rule for applications

1. In the type system:

\[(\text{APPL})\]

\[
\begin{align*}
\Gamma &\vdash e_1 : s \rightarrow u \\
\Gamma &\vdash e_2 : s \\
\hline
\Gamma &\vdash e_1 e_2 : u
\end{align*}
\]

[The type of the function is subsumed to an arrow and the type of the argument is subsumed to the domain of this arrow].

2. Subsumption elimination:

\[(\text{APPL-ALGORITHM})\]

\[
\begin{align*}
\Gamma &\vdash_{\mathcal{A}} e_1 : t \\
\Gamma &\vdash_{\mathcal{A}} e_2 : s \\
\hline
\Gamma &\vdash_{\mathcal{A}} e_1 e_2 : \min\{u \mid t \leq s \rightarrow u\} \\
&\text{subject to:} \\
t \leq 0 \rightarrow 1 \quad s \leq \text{dom}(t)
\end{align*}
\]
The rule for applications

1. In the type system:

\[(\text{APPL})\]
\[
\Gamma \vdash e_1 : s \rightarrow u \quad \Gamma \vdash e_2 : s
\]
\[
\Gamma \vdash e_1 e_2 : u
\]

[The type of the function is subsumed to an arrow and the type of the argument is subsumed to the domain of this arrow].

2. Subsumption elimination:

\[(\text{APPL-ALGORITHM})\]
\[
\Gamma \vdash \mathcal{A} e_1 : t \quad \Gamma \vdash \mathcal{A} e_2 : s
\]
\[
\Gamma \vdash \mathcal{A} e_1 e_2 : \min\{u \mid t \leq s \rightarrow u\}
\]
\[
t \leq 0 \rightarrow 1
\]
\[
s \leq \text{dom}(t)
\]

3. Inference of type substitutions

\[(\text{APPL-INFERENCE})\]
\[
\exists [\sigma_i]_{i \in I}, [\sigma'_j]_{j \in J} \quad \Gamma \vdash I e_1 : t \quad \Gamma \vdash I e_2 : s
\]
\[
\Gamma \vdash I e_1 e_2 : \min\{u \mid t[\sigma'_j]_{j \in J} \leq s[\sigma_i]_{i \in I} \rightarrow u\}
\]
\[
t[\sigma'_j]_{j \in J} \leq 0 \rightarrow 1
\]
\[
s[\sigma_i]_{i \in I} \leq \text{dom}(t[\sigma'_j]_{j \in J})
\]

[ where $t[\sigma_i]_{i \in I} \overset{\text{def}}{=} \bigvee_{i \in I} t\sigma_i$ ]
The rule for applications

1. In the type system:

(\text{APPL})
\[\begin{align*}
\Gamma \vdash e_1 : s \rightarrow u \\
\Gamma \vdash e_2 : s
\end{align*}\]
\[\Gamma \vdash e_1 e_2 : u\]

[The type of the function is subsumed to an arrow and the type of the argument is subsumed to the domain of this arrow].

2. Subsumption elimination:

(\text{APPL-ALGORITHM})
\[\begin{align*}
\Gamma \vdash_{\mathcal{A}} e_1 : t \\
\Gamma \vdash_{\mathcal{A}} e_2 : s
\end{align*}\]
\[\Gamma \vdash_{\mathcal{A}} e_1 e_2 : \min\{u \mid t \leq s \rightarrow u\}\]
\[t \leq 0 \rightarrow 1\]
\[s \leq \text{dom}(t)\]

3. Inference of type substitutions

(\text{APPL-INFERENECE})
\[\begin{align*}
\exists [\sigma_i]_{i \in I}, [\sigma'_j]_{j \in J}
\Gamma \vdash_I e_1 : t \\
\Gamma \vdash_I e_2 : s
\end{align*}\]
\[\Gamma \vdash_I e_1 e_2 : \min\{u \mid t[\sigma'_j]_{j \in J} \leq s[\sigma_i]_{i \in I} \rightarrow u\}\]
\[t[\sigma'_j]_{j \in J} \leq 0 \rightarrow 1\]
\[s[\sigma_i]_{i \in I} \leq \text{dom}(t[\sigma'_j]_{j \in J})\]

[ where \(t[\sigma_i]_{i \in I} \equiv \bigvee_{i \in I} t\sigma_i\) ]
Tallying problem

The problem of inferring the type of an application is thus to find for $s$ and $t$ given, two sets $[\sigma_i]_{i \in I}, [\sigma_j]_{j \in J}$ such that:

$$t[\sigma_j]_{j \in J} \leq 0 \rightarrow 1 \quad \text{and} \quad s[\sigma_i]_{i \in I} \leq \text{dom}(t[\sigma_j]_{j \in J})$$
Tallying problem

The problem of inferring the type of an application is thus to find for \( s \) and \( t \) given, two sets \([\sigma_i]_{i \in I}, [\sigma'_j]_{j \in J}\) such that:

\[
t[\sigma'_j]_{j \in J} \leq 0 \rightarrow 1 \quad \text{and} \quad s[\sigma_i]_{i \in I} \leq \text{dom}(t[\sigma'_j]_{j \in J})
\]

This can be reduced to solving a suite of tallying problems:

**Definition (Type tallying)**

Let \( s \) and \( t \) be two types. A type-substitution \( \sigma \) is a solution for the tallying of \((s, t)\) iff \( s\sigma \leq t\sigma \).
The problem of inferring the type of an application is thus to find for \( s \) and \( t \) given, two sets \([\sigma_i]_{i \in I}, [\sigma'_j]_{j \in J}\) such that:

\[
\begin{align*}
  t[\sigma'_j]_{j \in J} &\leq 0 \rightarrow 1 \quad \text{and} \\
  s[\sigma_i]_{i \in I} &\leq \text{dom}(t[\sigma'_j]_{j \in J})
\end{align*}
\]

This can be reduced to solving a suite of tallying problems:

**Definition (Type tallying)**

Let \( s \) and \( t \) be two types. A type-substitution \( \sigma \) is a solution for the tallying of \((s, t)\) iff \( s\sigma \leq t\sigma \).

**Generally:** let \( C = \{(s_1 \leq t_1), \ldots, (s_n \leq t_n)\} \) a constraint set. A type-substitution \( \sigma \) is a solution for the tallying of \( C \) iff \( s\sigma \leq t\sigma \) for all \((s \leq t) \in C\).
Tallying problem

The problem of inferring the type of an application is thus to find for \( s \) and \( t \) given, two sets \([\sigma_i]_{i \in I}, [\sigma'_j]_{j \in J}\) such that:

\[
t[\sigma'_j]_{j \in J} \leq 0 \rightarrow 1 \quad \text{and} \quad s[\sigma_i]_{i \in I} \leq \text{dom}(t[\sigma'_j]_{j \in J})
\]

This can be reduced to solving a suite of *tallying problems*:

**Definition (Type tallying)**

Let \( s \) and \( t \) be two types. A type-substitution \( \sigma \) is a solution for the *tallying* of \((s, t)\) iff \( s\sigma \leq t\sigma \).

**Generally:** let \( C = \{(s_1 \leq t_1), \ldots, (s_n \leq t_n)\} \) a constraint set. A type-substitution \( \sigma \) is a solution for the *tallying* of \( C \) iff \( s\sigma \leq t\sigma \) for all \((s \leq t) \in C\).

Type tallying is decidable and a sound and complete set of solutions for every tallying problem can be effectively found in **three simple steps**.
Step 1: Decompose constraints.
Use the set-theoretic decomposition rules to transform $C$ into a set of constraint sets whose constraints are of the form $\alpha \leq t$ or $t \leq \alpha$. 
Step 1: Decompose constraints.
Use the set-theoretic decomposition rules to transform \( C \) into a set of constraint sets whose constraints are of the form \( \alpha \leq t \) or \( t \leq \alpha \).

Example:
1. \( \{(s_1 \rightarrow t_1 \leq s_2 \rightarrow t_2)\} \leadsto \{(s_2 \leq \emptyset)\} \) or \( \{(s_2 \leq s_1), (t_1 \leq t_2)\} \)
Step 1: Decompose constraints.
Use the set-theoretic decomposition rules to transform $C$ into a set of constraint sets whose constraints are of the form $\alpha \leq t$ or $t \leq \alpha$.

Step 2: Merge constraints on the same variable.
- if $\alpha \leq t_1$ and $\alpha \leq t_2$ are in $C$, then replace them by $\alpha \leq t_1 \land t_2$;
- if $s_1 \leq \alpha$ and $s_2 \leq \alpha$ are in $C$, then replace them by $s_1 \lor s_2 \leq \alpha$;
Possibly decompose the new constraints generated by transitivity.

Example:
1. $\{(s_1 \rightarrow t_1 \leq s_2 \rightarrow t_2)\} \leadsto \{(s_2 \leq \emptyset)\}$ or $\{(s_2 \leq s_1), (t_1 \leq t_2)\}$
Step 1: Decompose constraints.
Use the set-theoretic decomposition rules to transform $C$ into a set of constraint sets whose constraints are of the form $\alpha \leq t$ or $t \leq \alpha$.

Step 2: Merge constraints on the same variable.
- if $\alpha \leq t_1$ and $\alpha \leq t_2$ are in $C$, then replace them by $\alpha \leq t_1 \land t_2$;
- if $s_1 \leq \alpha$ and $s_2 \leq \alpha$ are in $C$, then replace them by $s_1 \lor s_2 \leq \alpha$;
Possibly decompose the new constraints generated by transitivity.

Example:
1. $\{(s_1 \rightarrow t_1 \leq s_2 \rightarrow t_2)\} \leadsto \{(s_2 \leq \emptyset)\}$ or $\{(s_2 \leq s_1), (t_1 \leq t_2)\}$
2. $\{(\text{Int} \leq \alpha), (\text{Bool} \leq \alpha)\} \leadsto \{(\text{Int} \lor \text{Bool} \leq \alpha)\}$
Step 1: Decompose constraints.
Use the set-theoretic decomposition rules to transform $C$ into a set of constraint sets whose constraints are of the form $\alpha \leq t$ or $t \leq \alpha$.

Step 2: Merge constraints on the same variable.
- if $\alpha \leq t_1$ and $\alpha \leq t_2$ are in $C$, then replace them by $\alpha \leq t_1 \land t_2$;
- if $s_1 \leq \alpha$ and $s_2 \leq \alpha$ are in $C$, then replace them by $s_1 \lor s_2 \leq \alpha$;

Possibly decompose the new constraints generated by transitivity.

Step 3: Transform into a set of equations.
After Step 2 we have constraint-sets of the form $\{s_i \leq \alpha_i \leq t_i \mid i \in [1..n]\}$ where $\alpha_i$ are pairwise distinct.

1. select $s \leq \alpha \leq t$ and replace it by $\alpha = (s \lor \beta) \land t$ with $\beta$ fresh.
2. substitute $(s \lor \beta) \land t$ for all $\alpha$ in the other constraints of $C$
3. repeat with another constraint

Example:
1. $\{(s_1 \to t_1 \leq s_2 \to t_2)\} \leadsto \{(s_2 \leq \emptyset)\}$ or $\{(s_2 \leq s_1), (t_1 \leq t_2)\}$
2. $\{(\text{Int} \leq \alpha), (\text{Bool} \leq \alpha)\} \leadsto \{(\text{Int} \lor \text{Bool} \leq \alpha)\}$
Step 1: Decompose constraints.
Use the set-theoretic decomposition rules to transform \( C \) into a set of constraint sets whose constraints are of the form \( \alpha \leq t \) or \( t \leq \alpha \).

Step 2: Merge constraints on the same variable.
- if \( \alpha \leq t_1 \) and \( \alpha \leq t_2 \) are in \( C \), then replace them by \( \alpha \leq t_1 \wedge t_2 \);
- if \( s_1 \leq \alpha \) and \( s_2 \leq \alpha \) are in \( C \), then replace them by \( s_1 \lor s_2 \leq \alpha \);

Possibly decompose the new constraints generated by transitivity.

Step 3: Transform into a set of equations.
After Step 2 we have constraint-sets of the form \( \{ s_i \leq \alpha_i \leq t_i \mid i \in [1..n] \} \) where \( \alpha_i \) are pairwise distinct.

1. select \( s \leq \alpha \leq t \) and replace it by \( \alpha = (s \lor \beta) \wedge t \) with \( \beta \) fresh.
2. substitute \( (s \lor \beta) \wedge t \) for all \( \alpha \) in the other constraints of \( C \)
3. repeat with another constraint

Example:
1. \( \{ (s_1 \rightarrow t_1 \leq s_2 \rightarrow t_2) \} \ \leadsto \ \{ (s_2 \leq 0) \} \text{ or } \{ (s_2 \leq s_1), (t_1 \leq t_2) \} \)
2. \( \{ (\text{Int} \leq \alpha), (\text{Bool} \leq \alpha) \} \ \leadsto \ \{ (\text{Int} \lor \text{Bool} \leq \alpha) \} \)
3. \( \{ (\text{Int} \leq \alpha_1 \leq \text{Real}), (\alpha_2 \leq \alpha_1 \wedge \text{Int}) \} \ \leadsto \ \{ \alpha_1 = (\text{Int} \lor \beta) \wedge \text{Real}, (\alpha_2 = \text{Int}) \} \)
Step 1: Decompose constraints.
Use the set-theoretic decomposition rules to transform \( C \) into a set of constraint sets whose constraints are of the form \( \alpha \leq t \) or \( t \leq \alpha \).

Step 2: Merge constraints on the same variable.
- If \( \alpha \leq t_1 \) and \( \alpha \leq t_2 \) are in \( C \), then replace them by \( \alpha \leq t_1 \land t_2 \);
- If \( s_1 \leq \alpha \) and \( s_2 \leq \alpha \) are in \( C \), then replace them by \( s_1 \lor s_2 \leq \alpha \);

Possibly decompose the new constraints generated by transitivity.

Step 3: Transform into a set of equations.
After Step 2 we have constraint-sets of the form \( \{ s_i \leq \alpha_i \leq t_i \mid i \in [1..n] \} \) where \( \alpha_i \) are pairwise distinct.
1. select \( s \leq \alpha \leq t \) and replace it by \( \alpha = (s \lor \beta) \land t \) with \( \beta \) fresh.
2. substitute \( (s \lor \beta) \land t \) for all \( \alpha \) in the other constraints of \( C \)
3. repeat with another constraint

At the end we have a sets of equations \( \{ \alpha_i = u_i \mid i \in [1..n] \} \) that (with some care) are contractive. By Courcelle there exists a solution, ie, a substitution for \( \alpha_1, \ldots, \alpha_n \) into (possibly recursive regular) types \( t_1, \ldots, t_n \) (in which the fresh \( \beta \)'s are free variables).
Example: map even

Start with the following tallying problem:

$$(\alpha_1 \rightarrow \beta_1) \rightarrow [\alpha_1] \rightarrow [\beta_1] \leq s \rightarrow \gamma$$

where $s = (\text{Int} \rightarrow \text{Bool}) \wedge (\alpha\backslash\text{Int} \rightarrow \alpha\backslash\text{Int})$ is the type of even
Example: \texttt{map even}

Start with the following tallying problem:

\[(\alpha_1 \rightarrow \beta_1) \rightarrow [\alpha_1] \rightarrow [\beta_1] \leq s \rightarrow \gamma\]

where \(s = (\text{Int} \rightarrow \text{Bool}) \land (\alpha \upharpoonright \text{Int} \rightarrow \alpha \upharpoonright \text{Int})\) is the type of \texttt{even}

- The algorithm generates 9 constraint-sets: one is unsatisfiable \((s \leq \emptyset)\); four are implied by the others; remain
  \[\{\gamma \geq [\alpha_1] \rightarrow [\beta_1], \alpha_1 \leq \emptyset\}, \{\gamma \geq [\alpha_1] \rightarrow [\beta_1], \alpha_1 \leq \text{Int}, \text{Bool} \leq \beta_1\},\]
  \[\{\gamma \geq [\alpha_1] \rightarrow [\beta_1], \alpha_1 \leq \alpha \upharpoonright \text{Int}, \alpha \upharpoonright \text{Int} \leq \beta_1\},\]
  \[\{\gamma \geq [\alpha_1] \rightarrow [\beta_1], \alpha_1 \leq \alpha \lor \text{Int}, (\alpha \upharpoonright \text{Int}) \lor \text{Bool} \leq \beta_1\};\]
Example: \texttt{map even}

Start with the following tallying problem:

\[(\alpha_1 \to \beta_1) \to [\alpha_1] \to [\beta_1] \leq s \to \gamma\]

where \(s = (\text{Int} \to \text{Bool}) \land (\alpha \setminus \text{Int} \to \alpha \setminus \text{Int})\) is the type of \texttt{even}

- The algorithm generates 9 constraint-sets: one is unsatisfiable \((s \leq \emptyset)\); four are implied by the others; remain

  \[
  \{\gamma \geq [\alpha_1] \to [\beta_1], \alpha_1 \leq \emptyset\}, \{\gamma \geq [\alpha_1] \to [\beta_1], \alpha_1 \leq \text{Int}, \text{Bool} \leq \beta_1\},
  \{\gamma \geq [\alpha_1] \to [\beta_1], \alpha_1 \leq \alpha \setminus \text{Int}, \alpha \setminus \text{Int} \leq \beta_1\},
  \{\gamma \geq [\alpha_1] \to [\beta_1], \alpha_1 \leq \alpha \lor \text{Int}, (\alpha \setminus \text{Int}) \lor \text{Bool} \leq \beta_1\};
  \]

- Four solutions for \(\gamma\):

  \[
  \{\gamma = [] \to []\},
  \{\gamma = [\text{Int}] \to [\text{Bool}]\},
  \{\gamma = [\alpha \setminus \text{Int}] \to [\alpha \setminus \text{Int}]\},
  \{\gamma = [\alpha \lor \text{Int}] \to [(\alpha \setminus \text{Int}) \lor \text{Bool}]\}.
  \]
Example: map even

Start with the following tallying problem:

\[(\alpha_1 \to \beta_1) \to [\alpha_1] \to [\beta_1] \leq s \to \gamma\]

where \(s = (\text{Int} \to \text{Bool}) \land (\alpha \mid \text{Int} \to \alpha \mid \text{Int})\) is the type of \text{even}

- The algorithm generates 9 constraint-sets: one is unsatisfiable \((s \leq 0)\); four are implied by the others; remain

  \[
  \begin{align*}
  \{\gamma \geq [\alpha_1] \to [\beta_1], \alpha_1 \leq 0\}, & \quad \{\gamma \geq [\alpha_1] \to [\beta_1], \alpha_1 \leq \text{Int}, \text{Bool} \leq \beta_1\}, \\
  \{\gamma \geq [\alpha_1] \to [\beta_1], \alpha_1 \leq \alpha \mid \text{Int}, \alpha \mid \text{Int} \leq \beta_1\}, & \quad \{\gamma \geq [\alpha_1] \to [\beta_1], \alpha_1 \leq \alpha \lor \text{Int}, (\alpha \mid \text{Int}) \lor \text{Bool} \leq \beta_1\};
  \end{align*}
  \]

- Four solutions for \(\gamma\):

  \[
  \begin{align*}
  \{\gamma = [] \to []\}, & \quad \{\gamma = [\text{Int}] \to [\text{Bool}]\}, \\
  \{\gamma = [\alpha \mid \text{Int}] \to [\alpha \mid \text{Int}]\}, & \quad \{\gamma = [\alpha \lor \text{Int}] \to [(\alpha \mid \text{Int}) \lor \text{Bool}]\}. 
  \end{align*}
  \]

- The last two are minimal and we take their intersection:

  \[
  \{\gamma = ([\alpha \mid \text{Int}] \to [\alpha \mid \text{Int}]) \land ([\alpha \lor \text{Int}] \to [(\alpha \mid \text{Int}) \lor \text{Bool}])\}
  \]
The algorithm produces a set of solutions that is **sound** (it finds only correct solutions) and **complete** (any other solution can be derived from them).
The algorithm produces a set of solutions that is **sound** (it finds only correct solutions) and **complete** (any other solution can be derived from them).

**Decidability:** The algorithm is a semi-decision procedure. We conjecture decidability (N.B.: the problem is unrelated to type-reconstruction for intersection types since we have *recursive types*).
The algorithm produces a set of solutions that is **sound** (it finds only correct solutions) and **complete** (any other solution can be derived from them).

**Decidability:** The algorithm is a semi-decision procedure. We conjecture decidability (N.B.: the problem is unrelated to type-reconstruction for intersection types since we have *recursive types*).

**Completeness:** For every solution of the inference problem, our algorithm finds an equivalent or more general solution. However, this solution is not necessary the first solution found.

In a dully execution of the algorithm on `map even` the good solution is the second one.
The algorithm produces a set of solutions that is **sound** (it finds only correct solutions) and **complete** (any other solution can be derived from them).

**Decidability:** The algorithm is a semi-decision procedure. We conjecture decidability (N.B.: the problem is unrelated to type-reconstruction for intersection types since we have *recursive types*).

**Completeness:** For every solution of the inference problem, our algorithm finds an equivalent or more general solution. However, this solution is not necessary the first solution found.

In a dully execution of the algorithm on `map even` the good solution is the second one.

**Principality:** This raises the problem of the existence of principal types: may an infinite sequence of increasingly general solutions exist?
References

  Reference publication for monomorphic semantic subtyping.

  A simple introduction to semantic subtyping and a detailed description of the implementation of subtyping and type-checking algorithms.

  Subtyping for polymorphic set-theoretic types

- Castagna et al.: *Polymorphic Functions with Set-Theoretic Types*. Part 1 (POPL 14) and Part 2 (POPL 15).
  Languages with polymorphic set-theoretic types

  Type reconstruction for polymorphic set-theoretic types
To try it out

- For polymorphism use the development branch available at https://gitlab.math.univ-paris-diderot.fr/cduce)
- For a flavor of type reconstruction try the interactive interpreter at http://www.cduce.org/ocaml/bi
Gradual Typing
Outline

15 Main ideas

16 Formal system

17 Algorithmic Aspects

18 Criteria for Gradual Typing

19 Implementation issues

20 References
Outline

15 Main ideas

16 Formal system

17 Algorithmic Aspects

18 Criteria for Gradual Typing

19 Implementation issues

20 References
function double (x ) {
  (\text{<condition>}) \ ? 2*x : x.concat(x)
}

Cannot give a type to \textit{x} that works with both 2\textit{x} and \textit{x}.concat(\textit{x})
Motivating example: reminder

```javascript
function double (x : ?) {
  (<condition>) ? 2*x : x.concat(x)
}
```

Cannot give a type to `x` that works with both `2*x` and `x.concat(x)`

**Solution**

Add an unknown/type “?”
Motivating example: reminder

function double (x : ?) {
    (>condition>) ? 2*x : x.concat(x)
}

Cannot give a type to x that works with both 2*x and x.concat(x)

Solution

Add an unknown/type “?”

Develop a type theory for “?” such that:

- No solution for ? for some execution $\Rightarrow$ statically reject
- No problem for any solution for ? $\Rightarrow$ statically accept, do nothing
- For each possible execution there exists some solution for ? $\Rightarrow$ statically accept and add run-time checks
Reject at compile time:

```javascript
function wrong (x : ?) {
  return (2*x + x(2));  //cannot be a number and a function
}
```

Accept as is:

```javascript
function ok (x : ?) {
  if (typeof(x) === "number"){ return 42 } else { return x }
}
```

Intuitively the function has type:

```latex
??? \rightarrow (\text{number} | ???)
```

Accept and insert checks:

```javascript
function double (x : ?) {
  (<condition>) ? 2*x : x.concat(x)
}
```

Compile as:

```javascript
function double (x : ?) {
  (<condition>) ? 2*(x \langle\text{number}\rangle) : (x \langle\text{string}\rangle).concat(x \langle\text{string}\rangle)
}
```
Reject at compile time:

```javascript
function wrong (x : ?) {
    return (2*x + x(2));   //cannot be a number and a function
}
```

Accept as is:

```javascript
function ok (x : ?) {
    if (typeof(x) === "number") { return 42 } else { return x }
}
```

Intuitively the function has type: `? → (number | ?)`
Reject at compile time:

```javascript
function wrong (x : ?) {
    return (2*x + x(2)); //cannot be a number and a function
}
```

Accept as is:

```javascript
function ok (x : ?) {
    if (typeof(x) === "number") { return 42 } else { return x }
}
```

Intuitively the function has type: `? → (number | ?)`

Accept and insert checks:

```javascript
function double (x : ?) {
    (<condition>) ? 2*x : x.concat(x)
}
```

Compile as

```javascript
function double (x : ?) {
    (<condition>) ? 2*(x<number>) : (x<string>).concat(x<string>)
}
```
Mix static and dynamic typing
Mix static and dynamic typing

```javascript
function double (x : ?) {
    (condition) ? 2*x : x.concat(x)
}

function apply (f : number --> number, x : number) {
    return (f x);
}

apply (double , (double 42))
```
Mix static and dynamic typing

Dynamically typed:

```javascript
function double (x : ?) {
  (<condition>) ? 2*x : x.concat(x)
}
```

Statically typed:

```javascript
function apply (f : number --> number, x : number) {
  return (f x);
}
```

Mixed typing:

```javascript
apply (double , (double 42))
```
Mix static and dynamic typing

Dynamically typed:
function double (x : ?) {
  (<condition>) ? 2*x : x.concat(x)
}

Statically typed:
function apply (f : number --> number, x : number) {
  return (f x);
}

Mixed typing:
apply (double , (double 42))

Add checks at the boundaries:
apply (double , (double 42))
must be compiled as
apply (double<number→number> , (double 42)<number>)
A hot topic

Prominent Languages with Gradual Typing:

- Typed Racket
- Reticulated Python
- TypeScript (Microsoft)
- Flow (Facebook)
- Hack (Facebook)
- Dart (Google)
- Thorn
- Safe Typescript
A hot topic

Prominent Languages with Gradual Typing:
- Typed Racket
- Reticulated Python
- TypeScript (Microsoft)
- Flow (Facebook)
- Hack (Facebook)
- Dart (Google)
- Thorn
- Safe Typescript

- Retrofitted on existing languages
- New languages
A hot topic

Prominent Languages with Gradual Typing:

- Typed Racket
- Reticulated Python
- TypeScript (Microsoft)
- Flow (Facebook)
- Hack (Facebook)
- Dart (Google)
- Thorn
- Safe Typescript

- Retrofitted on existing languages
- New languages

- Insert checks at run-time (a.k.a. sound gradual typing)
- Permissive typing (no checks inserted)
- Strict typing
- Occurrence typing
Roadmap

1. Add “?” to types

2. Define a typing discipline for programs with “?”
   - A well-typed program must still be well-typed with less-precise annotations
   - Less-precise annotations may make a program to become well-typed

3. Use the typing derivation to add dynamic type-checks at the boundaries between statically-type and dynamically-typed parts
   - Using less precise annotations in a well-typed program must not yield failures of dynamic checks (preserve semantics)
   - Failures of dynamic checks are due only to the dynamically-typed parts

Type precision: the lesser the “?”, the more precise the type.
Simply-typed $\lambda$-calculus types:

\[
\begin{align*}
\textit{Types} & \quad T & ::= & \text{Bool} & | & \text{Int} & | & T \rightarrow T \\
\end{align*}
\]
Simply-typed $\lambda$-calculus types:

\begin{align*}
\text{Types} & \quad T ::= \text{Bool} \mid \text{Int} \mid T \rightarrow T
\end{align*}
Gradual Typing

Simply-typed λ-calculus types:

\[ Types \quad T ::= \text{Bool} \mid \text{Int} \mid T \rightarrow T \mid ? \]

A new **consistency** relation “∼” governs implicit casts involving “?”:

\[
\begin{align*}
\text{Bool} \sim \text{Bool} & \quad \text{Int} \sim \text{Int} & \quad T \sim ? & \quad ? \sim T \\
S_1 \sim T_1 & \quad S_2 \sim T_2 & \quad S_1 \rightarrow S_2 \sim T_1 \rightarrow T_2
\end{align*}
\]
Gradual Typing

Simply-typed $\lambda$-calculus types:

$$Types \quad T ::= \text{Bool} \mid \text{Int} \mid T \rightarrow T \mid ?$$

A new **consistency** relation “$\sim$” governs implicit casts involving “?”:

- $\text{Bool} \sim \text{Bool}$
- $\text{Int} \sim \text{Int}$
- $T \sim ?$
- $? \sim T$
- $S_1 \sim T_1$  $S_2 \sim T_2$  $S_1 \rightarrow S_2 \sim T_1 \rightarrow T_2$

Relax application for consistent types:

$$[\rightarrow E\text{LIM}_\sim] \quad \Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : U \quad U \sim S$$

$$\Gamma \vdash ab : T$$
Simply-typed λ-calculus types:

Types \( T \) ::= Bool \mid Int \mid T \to T \mid ?

A new **consistency** relation “∼” governs implicit casts involving “?”:

\[
\begin{align*}
\text{Bool} \sim \text{Bool} & \quad \text{Int} \sim \text{Int} & \quad T \sim ? & \quad ? \sim T & \quad S_1 \sim T_1 & \quad S_2 \sim T_2 \\
\frac{}{S_1 \to S_2 \sim T_1 \to T_2}
\end{align*}
\]

Relax application for consistent types:

\[
\begin{align*}
\frac{\Gamma \vdash a : S \to T \quad \Gamma \vdash b : U \quad U \sim S}{\Gamma \vdash ab : T}
\end{align*}
\]

Use the type derivation to insert casts

\[
\begin{align*}
\frac{\Gamma \vdash a : S \to T \quad \text{compiles} \quad \Gamma \vdash b : U \quad \text{compiles} \quad U \sim S}{\Gamma \vdash ab : T \quad \text{compiles} \quad a(b\langle S\rangle)}
\end{align*}
\]
Simply-typed $\lambda$-calculus types:

$$Types \quad T \ ::= \ Bool \mid Int \mid T \to T \mid ?$$

A new **consistency** relation “$\sim$” governs implicit casts involving “?”:

\[
\begin{array}{cccc}
\text{Bool$\sim$Bool} & \text{Int$\sim$Int} & T \sim ? & ? \sim T \\
S_1 \sim T_1 & S_2 \sim T_2 & S_1 \to S_2 \sim T_1 \to T_2
\end{array}
\]

Relax application for consistent types:

\[
[\to E\text{LIM}_\sim] \quad \frac{\Gamma \vdash a : S \to T \quad \Gamma \vdash b : U \quad U \sim S}{\Gamma \vdash ab : T}
\]

Use the type derivation to insert casts

\[
[\to E\text{LIM}_\sim] \quad \frac{\Gamma \vdash a : S \to T \quad \text{compiles} \quad a'}{\Gamma \vdash ab : T \quad \text{compiles} \quad a(b(S)) \quad (U \not\equiv S)}
\]
Gradual Typing

Simply-typed $\lambda$-calculus types:

$$Types \quad T ::= \text{Bool} \mid \text{Int} \mid T \to T \mid ?$$

A new **consistency** relation "\(\sim\)" governs implicit casts involving "\(?\):

$$\begin{array}{cccccc}
\text{Bool} & \sim & \text{Bool} \\
\text{Int} & \sim & \text{Int} \\
T & \sim & ? \\
? & \sim & T \\
S_1 & \sim & T_1 \\
S_2 & \sim & T_2 \\
S_1 \to S_2 & \sim & T_1 \to T_2
\end{array}$$

Relax application for consistent types:

$$\Gamma \vdash a : S \to T \quad \Gamma \vdash b : U \quad \Gamma \vdash ab : T$$

Use the type derivation to insert casts:

$$\Gamma \vdash a : S \to T \quad \Gamma \vdash b : U \quad \Gamma \vdash ab : T$$

(U \neq S)
The consistency relation must not be transitive:

Since \(\text{Int} \sim ?\) and \(? \sim \text{Bool}\), then transitivity would imply \(\text{Int} \sim \text{Bool}\):

\[
\vdash \lambda x : \text{Int}. x + 1 : \text{Int} \rightarrow \text{Int} \quad \vdash \text{true} : \text{Bool} \quad \text{Int} \sim \text{Bool}
\]

\[
\vdash (\lambda x : \text{Int}. x + 1) \text{true} : \text{Int}
\]

It is hard to work with a non-transitive relation.
Problems

- **The consistency relation** *must not be transitive*: Since $\text{Int} \sim ?$ and $? \sim \text{Bool}$, then transitivity would imply $\text{Int} \sim \text{Bool}$:

\[
\vdash \lambda x : \text{Int}. x + 1 : \text{Int} \rightarrow \text{Int} \quad \vdash \text{true} : \text{Bool} \quad \text{Int} \sim \text{Bool}
\]

\[
\vdash (\lambda x : \text{Int}. x + 1) \text{true} : \text{Int}
\]

it is hard to work with a non-transitive relation.

- **It has a flavor of substitutivity ... but not always:**

function double (x : ?) { (<condition>) ? 2*x : x.concat(x) }

function apply (f : number --> number, x : number) { return (f x) }

apply (double, (double 42))

It compiles as apply (double⟨Int → Int⟩, (double⟨42⟩⟨?⟩)⟨Int⟩)
Problems

- The consistency relation **must not be transitive:**
Since \( \text{Int} \sim ? \) and \( ? \sim \text{Bool} \), then transitivity would imply \( \text{Int} \sim \text{Bool} \):

\[
\begin{align*}
\Gamma & \vdash \lambda x : \text{Int}.x + 1 : \text{Int} \rightarrow \text{Int} \quad \Gamma & \vdash \text{true} : \text{Bool} \\
\hline
\Gamma & \vdash (\lambda x : \text{Int}.x + 1)\text{true} : \text{Int}
\end{align*}
\]

It is hard to work with a non-transitive relation.

- It has a flavor of substitutivity ... but not always:

```javascript
function double (x : ?) { (<condition>) ? 2*x : x.concat(x) }
function apply (f : number --> number, x : number) { return (f x) }
apply (double , (double 42))
```

It compiles as

```javascript
apply ( double(\text{Int} \rightarrow \text{Int}) , (\text{double}(42⟨?⟩))(\text{Int}) )
```

- Casting \( ? \rightarrow ? \) to \( \text{Int} \rightarrow \text{Int} \) is ok.
The consistency relation **must not be transitive:**

Since \( \text{Int} \sim ? \) and \( ? \sim \text{Bool} \), then transitivity would imply \( \text{Int} \sim \text{Bool} \):

\[
\begin{align*}
\vdash \lambda x : \text{Int}.x + 1 : \text{Int} \rightarrow \text{Int} & \quad \vdash \text{true} : \text{Bool} \quad \text{Int} \sim \text{Bool} \\
\vdash (\lambda x : \text{Int}.x + 1) \text{true} : \text{Int}
\end{align*}
\]

It is hard to work with a non-transitive relation.

It has a flavor of substitutivity ... but not always:

```javascript
function double (x : ?) { (<condition>) ? 2*x : x.concat(x) }
function apply (f : number --> number, x : number) { return (f x) }
apply (double , (double 42))
```

It compiles as

\[
\text{apply} \ (\text{double} \langle \text{Int} \rightarrow \text{Int} \rangle , (\text{double}(42\langle ? \rangle))\langle \text{Int} \rangle)
\]

- Casting \(? \rightarrow ?\) to \text{Int} \rightarrow \text{Int} is ok.
- Casting \(? \) to \text{Int} is ok.
The consistency relation **must not be transitive:**
Since Int\(\sim ?\) and ?\(\sim\)Bool, then transitivity would imply Int\(\sim\)Bool:

\[
\begin{align*}
\vdash & \lambda x : \text{Int}. x + 1 : \text{Int} \rightarrow \text{Int} & \vdash & \text{true} : \text{Bool} & \text{Int} \sim \text{Bool} \\
\vdash & (\lambda x : \text{Int}. x + 1) \text{true} : \text{Int}
\end{align*}
\]

It is hard to work with a non-transitive relation.

It has a flavor of substitutivity ... but not always:

function double (x : ?) { (<condition>) ? 2\*x : x.concat(x) }
function apply (f : number \rightarrow\text{number}, x : number) { return (f x) }
apply (double , (double 42))

It compiles as  
apply ( double\langle\text{Int} \rightarrow \text{Int}\rangle , (double(42\langle?\rangle))\langle\text{Int}\rangle )

- Casting \(?\rightarrow\?) to \text{Int} \rightarrow \text{Int} is ok.
- Casting \(?\) to \text{Int} is ok.
- Casting an \text{Int} to \? looks weird
The \([\to \text{ELIM}\sim]\) rule looks more an algorithmic step than a typing rule:

\[
\begin{align*}
\Gamma \vdash a : S \to T \quad \Gamma \vdash b : U \quad U \sim S \\
\Gamma \vdash ab : T \\
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash \mathcal{A} a : S \to T \quad \Gamma \vdash \mathcal{A} b : U \quad U \leq S \\
\Gamma \vdash \mathcal{A} ab : T \\
\end{align*}
\]
The \(\rightarrow \text{ELIM} \sim\) rule looks more an algorithmic step than a typing rule:

\[
\begin{align*}
\frac{
\Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : U \quad U \sim S
}{
\Gamma \vdash ab : T
}\end{align*}
\]

\[
\begin{align*}
\frac{
\Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : U \quad U \leq S
}{
\Gamma \vdash a b : T
}\end{align*}
\]

We need a more principled methodology
The $[\to \text{ELIM}_{\sim}]$ rule looks more an algorithmic step than a typing rule:

\[
\begin{align*}
[\to \text{ELIM}_{\sim}] & \quad \Gamma \vdash a : S \to T \quad \Gamma \vdash b : U \quad U \sim S \\
& \quad \Gamma \vdash ab : T
\end{align*}
\]

\[
\begin{align*}
[\to \text{ELIM}_{\leq}] & \quad \Gamma \vdash_{A} a : S \to T \quad \Gamma \vdash_{A} b : U \quad U \leq S \\
& \quad \Gamma \vdash_{A} ab : T
\end{align*}
\]

We need a more principled methodology

Let’s take inspiration from what we did for subtyping
The precision relation "\(\sqsubseteq\)":
Precision relates a type with unknown "?" components to the types it may dynamically become at run time.
The precision relation “⊑”:
Precision relates a type with unknown “?” components to the types it may dynamically become at run time.

Informally

The less “?” it uses, the more precise a type is.
Precision and Materialization

The precision relation \(\sqsubseteq\):

Precision relates a type with unknown \(\text{“?”}\) components to the types it \textit{may} dynamically become at run time.

Informally

The less \(\text{“?”}\) it uses, the more \textit{precise} a type is.

Can be defined by induction for simple types:

\[
\begin{align*}
? \sqsubseteq T \\
S_1 \sqsubseteq T_1 & \quad S_2 \sqsubseteq T_2 \\
S_1 \rightarrow S_2 \sqsubseteq T_1 \rightarrow T_2 & \quad T \sqsubseteq T \\
T_1 \sqsubseteq T_2 & \quad T_2 \sqsubseteq T_3 \\
\end{align*}
\]
Precision and Materialization

**The precision relation “≦”:**
Precision relates a type with unknown “?” components to the types it may dynamically become at run time.

**Informally**

The less “?” it uses, the more precise a type is.

Can be defined by induction for simple types:

\[
\begin{align*}
? & \subseteq T \\
S_1 & \subseteq T_1 \\
S_2 & \subseteq T_2 \\
S_1 \rightarrow S_2 & \subseteq T_1 \rightarrow T_2 \\
T & \subseteq T \\
T_1 & \subseteq T_2 \\
T_2 & \subseteq T_3
\end{align*}
\]

- It is *not* subtyping
The precision relation “\(\sqsubseteq\)”:
Precision relates a type with unknown “?” components to the types it may dynamically become at run time.

Informally

The less “?” it uses, the more precise a type is.

Can be defined by induction for simple types:

\[
\begin{align*}
? & \sqsubseteq T \\
S_1 \sqsubseteq T_1 & \quad S_2 \sqsubseteq T_2 \\
S_1 \rightarrow S_2 \sqsubseteq T_1 \rightarrow T_2 & \\
T & \sqsubseteq T \\
T_1 \sqsubseteq T_2 & \quad T_2 \sqsubseteq T_3
\end{align*}
\]

- It is not subtyping
- It is a pre-order
Precision and Materialization

The precision relation “⊑”:
Precision relates a type with unknown “?” components to the types it may dynamically become at run time.

Informally
The less “?” it uses, the more precise a type is.

Can be defined by induction for simple types:

\[
\begin{align*}
? \subseteq T & \quad S_1 \subseteq T_1 \quad S_2 \subseteq T_2 \\
S_1 \rightarrow S_2 \subseteq T_1 \rightarrow T_2 & \quad T \subseteq T \quad T_1 \subseteq T_2 \subseteq T_3
\end{align*}
\]

- It is not subtyping
- It is a pre-order

Intuition

\( T \subseteq T' \) means that at run-time type \( T \) may turn out to be the type \( T' \).

we say that \( T \) may materialize into \( T' \)
The precision relation is a pre-order thus, in particular, it is *transitive*:

\[
? \sqsubseteq \ ? \rightarrow \ ? \sqsubseteq \ ? \rightarrow \text{Int} \sqsubseteq \ \text{Int} \rightarrow \text{Int}
\]
The precision relation is a pre-order thus, in particular, it is *transitive*:

\[
? \sqsubseteq ? \rightarrow ? \sqsubseteq ? \rightarrow \text{Int} \sqsubseteq \text{Int} \rightarrow \text{Int}
\]

but:

\[
? \sqsubseteq \text{Int} \nsubseteq ?
\]
The precision relation is a pre-order thus, in particular, it is *transitive*:

\[
? \sqsubseteq ? \rightarrow ? \sqsubseteq ? \rightarrow \text{Int} \sqsubseteq \text{Int} \rightarrow \text{Int}
\]

but:

\[
? \sqsubseteq \text{Int} \not\sqsubseteq ?
\]

This means that it can be used in a subsumption-like rule:

\[
\text{[MATERIALIZE] } \Gamma \vdash a : S \quad S \sqsubseteq T \quad \quad \Rightarrow \quad \Gamma \vdash a : T
\]
The precision relation is a pre-order thus, in particular, it is *transitive*:

\[
? \subseteq ? \rightarrow \ ? \subseteq \ ? \rightarrow \text{Int} \subseteq \text{Int} \rightarrow \text{Int}
\]

but:

\[
? \subseteq \text{Int} \not\subseteq ?
\]

This means that it can be used in a subsumption-like rule:

\[
\text{[MATERIALIZE]} \quad \frac{\Gamma \vdash a : S \quad S \subseteq T}{\Gamma \vdash a : T}
\]

We can add it to any type system to embed gradual typing in it.
The precision relation is a pre-order thus, in particular, it is *transitive*:

\[
\begin{align*}
? \sqsubseteq ? \rightarrow ? & \sqsubseteq ? \rightarrow \text{Int} \sqsubseteq \text{Int} \rightarrow \text{Int} \\
? \sqsubseteq \text{Int} & \nsubseteq \ ?
\end{align*}
\]

but:

\[
\begin{align*}
? \sqsubseteq \text{Int} & \nsubseteq ?
\end{align*}
\]

This means that it can be used in a subsumption-like rule:

\[
[MATERIALIZE] \quad \frac{\Gamma \vdash a : S \quad S \sqsubseteq T}{\Gamma \vdash a : T}
\]

We can add it to any type system to embed gradual typing in it.

**Rationale**

As *subtyping* captures "safe replacement", so *precision* captures "potential materialization".
Since *potential materialization* does not mean *assured* materialization, then we have to check it at run-time:

\[
\begin{align*}
\text{[MATERIALIZE]} \quad & \quad \Gamma \vdash a : S \xrightarrow{\text{compiles}} a' \quad S \subseteq T \\
\Gamma \vdash a : T & \xrightarrow{\text{compiles}} a'(T)
\end{align*}
\]
Since *potential materialization* does not mean *assured* materialization, then we have to check it at run-time:

\[
\frac{\Gamma \vdash a : S \text{ compiles} \quad S \subseteq T}{\Gamma \vdash a : T \text{ compiles} \quad a' \langle T \rangle}
\]

**Rationale**

- **Subtyping** = assured materialization (cast always works)
- **Precision** = possible materialization (cast may fail)
Since potential materialization does not mean assured materialization, then we have to check it at run-time:

\[
\frac{\Gamma \vdash a : S \overset{\text{compiles}}{\longrightarrow} a' \quad S \subseteq T}{\Gamma \vdash a : T \overset{\text{compiles}}{\longrightarrow} a'\langle T \rangle}
\]

Rationale

- **Subtyping** = assured materialization (cast always works)
- **Precision** = possible materialization (cast may fail)

From a logical viewpoint:

\[
\frac{\Gamma \vdash a : S \overset{\text{compiles}}{\longrightarrow} a' \quad S \leq T}{\Gamma \vdash a : T \overset{\text{compiles}}{\longrightarrow} a'\langle T \rangle}
\]

Subsumption as implicit coercions (subtyping)

\[
\frac{\Gamma \vdash a : S \overset{\text{compiles}}{\longrightarrow} a' \quad S \subseteq T}{\Gamma \vdash a : T \overset{\text{compiles}}{\longrightarrow} a'\langle T \rangle}
\]

Materialization as explicit casts (precision)
Summing up

Take your favorite typed language

Add "???",

Add the materialization rule (with suitable \(\sqsubseteq\)),

Compile to insert casts

Et voila: you have added gradual typing

Types

\[ T ::= \text{Int} \mid \text{Bool} \mid T \rightarrow T \mid ??? \]

Terms

\[ a, b ::= x \mid ab \mid \lambda x : T. a \mid 1 \mid 2 \mid \ldots \]

\[ (\lambda x : T. a) \rightarrow b \rightarrow a\left[ b / x \right] \]

\[ \Gamma \vdash x : \Gamma(x) \]

\[ \Gamma \vdash \lambda x : S. a : S \rightarrow T \]

\[ \Gamma \vdash a : S \rightarrow T \]

\[ \Gamma \vdash ab : T \]

\[ \Gamma \vdash a : S \sqsubseteq T \]

\[ \Gamma \vdash a : T \]

\[ \Gamma \vdash a : S \sqsubseteq T \]

Summing up

1. Take your favorite typed language
2. Add “?” to types
3. Add the materialization rule (with suitable \(\sqsubseteq\))
4. Compile to insert casts
5. Et voila: you have added gradual typing

Types \( T \) ::= \( \text{Int} \mid \text{Bool} \mid T \to T \)
Terms \( a, b \) ::= \( x \mid ab \mid \lambda x: T.a \mid 1 \mid 2 \mid ... \) \( (\lambda x: T.a)b \longrightarrow a[b/x] \)

\[ \frac{\Gamma, x : S \vdash a : T}{\Gamma \vdash x : \Gamma(x)} \quad \frac{\Gamma \vdash \lambda x : S.a : S \to T}{\Gamma \vdash \lambda x : S.a : S \to T} \quad \frac{\Gamma \vdash a : S \to T \quad \Gamma \vdash b : S}{\Gamma \vdash ab : T} \]
Summing up

1. Take your favorite typed language
2. Add “?” to types
3. Add the materialization rule (with suitable ⊑)
4. Compile to insert casts
5. Et voila: you have added gradual typing

Types

\[ T ::= \text{Int} \mid \text{Bool} \mid T \to T \]

Terms

\[ a, b ::= x \mid ab \mid \lambda x: T.a \mid 1 \mid 2 \mid \ldots \]

\[ (\lambda x: T.a)b \longrightarrow a[b/x] \]

\[
\begin{align*}
\text{[VAR]} & : \quad \Gamma, x : S \vdash a : T \\
\text{[\rightarrow \text{INTRO}]} & : \quad \Gamma \vdash x : \Gamma(x) \\
\text{[\rightarrow \text{ELIM}]} & : \quad \Gamma \vdash a : S \to T \quad \Gamma \vdash b : S \\
\end{align*}
\]
**Summing up**

1. Take your favorite typed language
2. Add “?” to types
3. Add the materialization rule (with suitable \( \sqsubseteq \))
4. Compile to insert casts
5. Et voila: you have added gradual typing

\[
\begin{align*}
\textit{Types} & \quad T ::= \text{Int} \mid \text{Bool} \mid T \rightarrow T \mid ? \\
\textit{Terms} & \quad a, b ::= x \mid ab \mid \lambda x : T . a \mid 1 \mid 2 \mid \ldots \quad (\lambda x : T . a) b \rightarrow a[b/x]
\end{align*}
\]

- [VAR] \( \Gamma \vdash x : \Gamma(x) \)
- [\( \rightarrow \text{INTRO} \)] \( \Gamma, x : S \vdash a : T \)
- [\( \rightarrow \text{ELIM} \)] \( \Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S \)
- \( \Gamma \vdash \lambda x : S . a : S \rightarrow T \)
- \( \Gamma \vdash ab : T \)

- [\( \rightarrow \text{MATERIALIZE} \)] \( \Gamma \vdash a : S \quad S \sqsubseteq T \)
  \( \Gamma \vdash a : T \)
Summing up

1. Take your favorite typed language
2. Add “?” to types
3. Add the materialization rule (with suitable \(\sqsubseteq\))
4. Compile to insert casts
5. Et voila: you have added gradual typing

**Types**

\[
T ::= \text{Int} \mid \text{Bool} \mid T \rightarrow T \mid ?
\]

**Terms**

\[
a, b ::= x \mid ab \mid \lambda x : T . a \mid 1 \mid 2 \mid ...
\]

\[
\Gamma \vdash x : \Gamma(x)
\]

\[
\Gamma, x : S \vdash a : T
\]

\[
\Gamma \vdash x : \Gamma(x)
\]

\[
\Gamma \vdash \lambda x : S . a : S \rightarrow T
\]

\[
\Gamma \vdash ab : T
\]

\[
\Gamma \vdash a : S \quad S \sqsubseteq T
\]

\[
\Gamma \vdash a : T
\]

\[
\Gamma \vdash a : S \quad \text{compiles} \quad a' \quad S \subseteq T
\]

\[
\Gamma \vdash a : T \quad \text{compiles} \quad a' \langle T \rangle
\]
Summing up

1. Take your favorite typed language
2. Add “?” to types
3. Add the materialization rule (with suitable ⊑)
4. Compile to insert casts
5. Et voila: you have added gradual typing

Types \[ T ::= \text{Int} \mid \text{Bool} \mid T \rightarrow T \mid ? \]
Terms \[ a, b ::= x \mid ab \mid \lambda x: T.a \mid 1 \mid 2 \mid ... \]

\[ (\lambda x: T.a)b \rightarrow a[b/x] \]

\[ \Gamma \vdash x : \Gamma(x) \]
\[ \Gamma \vdash \lambda x : S.a : S \rightarrow T \]
\[ \Gamma \vdash \lambda x : S.a : S \rightarrow T \]
\[ \Gamma \vdash ab : T \]

\[ \Gamma \vdash a : S \quad \Gamma \vdash a : T \]
\[ \Gamma \vdash a : S \quad \Gamma \vdash a : T \quad \text{compiles} \quad \Gamma \vdash a : T \]

\[ \Gamma \vdash x : S \quad \Gamma \vdash x : S \quad \Gamma \vdash x : T \]
\[ \Gamma \vdash x : S \quad \Gamma \vdash x : S \quad \Gamma \vdash x : T \]

\[ \Gamma \vdash a : T \quad \Gamma \vdash a : T \quad \text{compiles} \quad \Gamma \vdash a : T \]

\[ \Gamma \vdash a : S \quad \Gamma \vdash a : S \quad \Gamma \vdash a : T \]
\[ \Gamma \vdash a : S \quad \Gamma \vdash a : S \quad \Gamma \vdash a : T \]
Summing up

1. Take your favorite typed language
2. Add “?” to types
3. Add the materialization rule (with suitable ⊑)
4. Compile to insert casts
5. Et voila: you have added gradual typing

\[
\begin{align*}
\text{Types} & \quad T ::= \text{Int} \mid \text{Bool} \mid T \to T \mid ? \\
\text{Terms} & \quad a, b ::= x \mid ab \mid \lambda x:T.a \mid 1 \mid 2 \mid \ldots
\end{align*}
\]

\[
\begin{align*}
\text{[VAR]} & \quad \Gamma, x : S \vdash a : T \\
\text{[\rightarrow\text{INTRO}]} & \quad \Gamma \vdash a : S \to T \quad \Gamma \vdash b : S \\
\text{[\rightarrow\text{ELIM}]} & \quad \Gamma \vdash ab : T
\end{align*}
\]

\[
\begin{align*}
\text{[\text{MATERIALIZE}] } & \quad \Gamma \vdash a : S \quad S \subseteq T \\
\text{[\text{MATERIALIZE}_{\text{COMPIL}}]} & \quad \Gamma \vdash a : S \quad \text{compiles} \quad a' \quad S \subseteq T \\
\end{align*}
\]

Is it that simple?!?!
Summing up

1. Take your favorite typed language
2. Add “?” to types
3. Add the materialization rule (with suitable ⊑)
4. Compile to insert casts
5. Et voila: you have added gradual typing

Types

\[ T ::= \text{Int} \mid \text{Bool} \mid T \rightarrow T \mid ? \]

Terms

\[ a, b ::= x \mid ab \mid \lambda x: T.a \mid 1 \mid 2 \mid \ldots \]

\[ (\lambda x: T.a)b \rightarrow a[b/x] \]

\[
\begin{align*}
\text{[VAR]} & \quad \text{[\rightarrow\text{INTRO}]} & \quad \text{[\rightarrow\text{ELIM}]} \\
\Gamma \vdash x : \Gamma(x) & \quad \Gamma, x : S \vdash a : T & \quad \Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S \\
\Gamma \vdash \lambda x : S.a : S \rightarrow T & \quad \Gamma \vdash ab : T
\end{align*}
\]

\[
\begin{align*}
\text{[\text{MATERIALIZE}] } & \quad \text{[\text{MATERIALIZE}_{\text{COMPIL}}]} \\
\Gamma \vdash a : S & \quad S \subseteq T & \quad \Gamma \vdash a : T \\
\Gamma \vdash a : S \text{ \text{compiles}} & \quad a' & \quad S \subseteq T
\end{align*}
\]

\[
\Gamma \vdash a : T \text{ \text{compiles}} \quad a' \langle T \rangle
\]
Summing up

1. Take your favorite typed language
2. Add “？” to types
3. Add the materialization rule (with suitable \[\sqsubseteq\])
4. Compile to insert casts
5. Et voila: you have added gradual typing

\[
Types \quad T ::= \text{Int} \mid \text{Bool} \mid T \rightarrow T \mid ? \\
\text{Terms} \quad a, b ::= x \mid ab \mid \lambda x:T.a \mid 1 \mid 2 \mid ...
\]

\[
\text{[VAR] } \quad \text{[\rightarrow\text{INTRO}] } \quad \text{[\rightarrow\text{ELIM}] } \\
\quad \Gamma, x:S \vdash a:T \quad \Gamma, x:S \vdash \lambda x:S.a:S \rightarrow T \quad \Gamma \vdash a:S \rightarrow T \quad \Gamma \vdash b:S \\
\quad \Gamma \vdash x : \Gamma(x) \quad \Gamma \vdash \lambda x:S.a:S \rightarrow T \quad \Gamma \vdash ab:T
\]

\[
\text{[\text{MATERIALIZE}] } \quad \text{[\text{MATERIALIZE}_{\text{COMPIL}}]} \\
\quad \Gamma \vdash a:S \quad S \sqsubseteq T \\
\quad \Gamma \vdash a:T \\
\quad \Gamma \vdash a:T \quad \Gamma \vdash a:T \quad \text{compiles} \quad \text{compiles} \\
\quad \Gamma \vdash a':S \quad \Gamma \vdash a':\langle T \rangle \quad S \sqsubseteq T
\]
Summing up

1. Take your favorite typed language
2. Add “?” to types
3. Add the materialization rule (with suitable ⊑)
4. Compile to insert casts
5. Et voila: you have added gradual typing

Types $T ::= \text{Int} \mid \text{Bool} \mid T \to T \mid ?$

Terms $a, b ::= x \mid ab \mid \lambda x : T.a \mid 1 \mid 2 \mid ...$

YES!... as long as you don’t pretend to implement it!!!
Algorithmic aspects

From more theoretical to more practical ones:

- Materialization elimination: as we had to eliminate subsumption to get a type-checking algorithm so we have to do the same for \texttt{MATERIALIZE}.

- Implementation of casts: the implementation of the cast calculus is not trivial. How do we check casts? In particular, how do we handle functional casts: \((\text{double} \langle \text{Int} \rightarrow \text{Int} \rangle)(42) \rightarrow \text{???})

- Error messages: when a cast fails which part of the program is to blame?

- Efficient implementation: how to avoid accumulation of cast compositions (i.e., stack overflow) and how to implement efficiently tail recursion for functions with casts?

But before that, let me show you that the approach works and it is pretty general.
Algorithmic aspects

From more theoretical to more practical ones:

- **Materialization elimination**: as we had to eliminate subsumption to get a type-checking algorithm so we have to do the same for [MATERIALIZE].
Algorithmic aspects

From more theoretical to more practical ones:

- **Materialization elimination**: as we had to eliminate subsumption to get a type-checking algorithm so we have to do the same for [MATERIALIZE].

- **Implementation of casts**: the implementation of the cast calculus is not trivial. How do we check casts? In particular, how do we handle functional casts:

  \[(\text{double} \langle \text{Int} \rightarrow \text{Int} \rangle)(42) \rightarrow ???\]
Algorithmic aspects

From more theoretical to more practical ones:

- **Materialization elimination**: as we had to eliminate subsumption to get a type-checking algorithm so we have to do the same for \[\text{MATERIALIZE}\].

- **Implementation of casts**: the implementation of the cast calculus is not trivial. How do we check casts? In particular, how do we handle functional casts:

  \[
  (\text{double}\langle\text{Int} \to \text{Int}\rangle)(42) \rightarrow ???
  \]

- **Error messages**: when a cast fails which part of the program is to blame?
Algorithmic aspects

From more theoretical to more practical ones:

- **Materialization elimination**: as we had to eliminate subsumption to get a type-checking algorithm so we have to do the same for [MATERIALIZE].

- **Implementation of casts**: the implementation of the cast calculus is not trivial. How do we check casts? In particular, how do we handle functional casts:

  \[(\text{double}\langle\text{Int}\to\text{Int}\rangle)(42) \rightarrow ???\]

- **Error messages**: when a cast fails which part of the program is to blame?

- **Efficient implementation**: how to avoid accumulation of cast compositions (i.e., stack overflow) and how to implement efficiently tail recursion for functions with casts?
Algorithmic aspects

From more theoretical to more practical ones:

- **Materialization elimination**: as we had to eliminate subsumption to get a type-checking algorithm so we have to do the same for [MATERIALIZE].

- **Implementation of casts**: the implementation of the cast calculus is not trivial. How do we check casts? In particular, how do we handle functional casts:

  \[(\text{double}(\text{Int} \to \text{Int}))(42) \rightarrow ???\]

- **Error messages**: when a cast fails which part of the program is to blame?

- **Efficient implementation**: how to avoid accumulation of cast compositions (i.e., stack overflow) and how to implement efficiently tail recursion for functions with casts?

But before that, let me show you that the approach works and it is pretty general.
A principled approach

Simply Typed Lambda Calculus

Syntax:

Types \( T \) ::= Int | Bool | \( T \to T \)

Terms \( a, b \) ::= \( x \) | \( ab \) | \( \lambda x:T.a \) | 1 | 2 | ...

Semantics:

\[(\beta) (\lambda x:T.a)b \longrightarrow a[b/x]\]

Typing

\[\frac{\Gamma, x : S \vdash a : T}{\Gamma \vdash x : \Gamma(x)} \quad \frac{\Gamma \vdash \lambda x:S.a : S \to T}{\Gamma \vdash \lambda x: S.a : S \to T} \quad \frac{\Gamma \vdash a : S \to T \quad \Gamma \vdash b : S}{\Gamma \vdash ab : T}\]
A principled approach

Simply Typed Lambda Calculus

Syntax:

Types \( T \) ::= \( \text{Int} \mid \text{Bool} \mid T \rightarrow T \mid ? \)

Terms \( a, b \) ::= \( x \mid ab \mid \lambda x:T.a \mid 1 \mid 2 \mid ... \)

Semantics:

\((\beta)\) \quad (\lambda x:T.a)b \rightarrow a[b/x]

Typing

\[ \frac{}{\Gamma \vdash x : \Gamma(x)} \quad \frac{\Gamma \vdash \lambda x:S.a : S \rightarrow T}{\Gamma \vdash \lambda x:S.a : S \rightarrow T} \quad \frac{\Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S}{\Gamma \vdash ab : T} \quad \frac{}{\Gamma \vdash a : S \quad S \subseteq T}{\text{[MATERIALIZE]}} \]
A principled approach

Simply Typed Lambda Calculus

Syntax:

Types  \( T \) ::= Int | Bool | T → T | ?

Terms  \( a, b \) ::= x | ab | \( \lambda x:T.a \) | 1 | 2 | ...

Semantics:

\[(\beta) \quad (\lambda x:T.a)b \rightarrow a[b/x]\]

Typing

\[
\begin{align*}
\Gamma, x : S & \vdash a : T \\
\Gamma & \vdash x : \Gamma(x) \\
\Gamma & \vdash \lambda x : S.a : S \rightarrow T \\
\Gamma & \vdash a : S \rightarrow T \\
\Gamma, x : S & \vdash a : T \\
\Gamma \vdash b : S \\
\Gamma & \vdash ab : T \\
\end{align*}
\]

[MATERIALIZE] \[
\begin{align*}
\Gamma & \vdash a : S \\
S & \subseteq T \\
\Gamma & \vdash a : T \\
\end{align*}
\]
A principled approach

Simply Typed Lambda Calculus

Syntax:

\[\begin{align*}
  \text{Types} & \quad T ::= \text{Int} \mid \text{Bool} \mid T \to T \mid ? \\
  \text{Terms} & \quad a, b ::= x \mid ab \mid \lambda x:T.a \mid 1 \mid 2 \mid ...
\end{align*}\]

Semantics:

\[
\begin{array}{c}
\text{[MATERIALIZE}_\text{COMPIL}] \\
\frac{\Gamma \vdash a : S \quad \text{compiles} \quad a' \quad S \subseteq T}{\Gamma \vdash a : T \quad \text{compiles} \quad a'(T)}
\end{array}
\]

Typing

\[
\begin{align*}
  &\frac{\Gamma, x : S \vdash a : T}{\Gamma \vdash x : \Gamma(x)} \\
  &\frac{\Gamma \vdash \lambda x:S.a : S \to T}{\Gamma \vdash \lambda x:S.a : S \to T} \\
  &\frac{\Gamma \vdash a : S \to T \quad \Gamma \vdash b : S}{\Gamma \vdash ab : T} \\
  &\frac{\Gamma \vdash a : S \quad S \subseteq T}{\Gamma \vdash a : T}
\end{align*}
\]
A principled approach

Simply Typed Lambda Calculus + Gradual Typing

Syntax:

Types

\[ T :::= \text{Int} \mid \text{Bool} \mid T \rightarrow T \mid ? \]

Terms

\[ a, b :::= x \mid ab \mid \lambda x:T.a \mid 1 \mid 2 \mid ... \]

Semantics:

\[
\begin{align*}
\text{[MATERIALIZE} & \text{COMPIL]} \quad \Gamma \vdash a : S \quad \text{compiles} \quad a' \\
& \quad S \subseteq T \\
\text{[MATERIALIZE]} \quad \Gamma \vdash a : T \quad \text{compiles} \quad a'\langle T \rangle
\end{align*}
\]

Typing

\[
\begin{align*}
\Gamma \vdash x : \Gamma(x) \\
\Gamma \vdash \lambda x:S.a : S \rightarrow T \\
\Gamma \vdash a : S \rightarrow T \\
\Gamma \vdash b : S \\
\Gamma \vdash ab : T \\
\text{[MATERIALIZE]} \quad \Gamma \vdash a : S\quad S \subseteq T \\
\Gamma \vdash a : T
\end{align*}
\]
A principled approach

**Simply Typed Lambda Calculus + Gradual Typing + Subtyping**

**Syntax:**
- Types:  \( T ::= \text{Int} \mid \text{Bool} \mid T \to T \mid ? \)
- Terms:  \( a, b ::= x \mid ab \mid \lambda x: T.a \mid 1 \mid 2 \mid ... \)

**Semantics:**
- \([\text{MATERIALIZE}_{\text{COMPIL}}]\)
  \[\frac{\Gamma \vdash a : S \quad \text{compiles} \quad a' \quad S \subseteq T}{\Gamma \vdash a : T \quad \text{compiles} \quad a' \langle T \rangle}\]

**Typing**
- \( \Gamma, x : S \vdash a : T \)
- \( \Gamma \vdash \lambda x : S.a : S \to T \)
- \( \Gamma \vdash a : S \to T \quad \Gamma \vdash b : S \)
  \( \Gamma \vdash ab : T \)
- \([\text{MATERIALIZE}]\)
  \( \frac{\Gamma \vdash a : S \quad S \subseteq T}{\Gamma \vdash a : T}\)
- \([\text{SUBSUM}]\)
  \( \frac{\Gamma \vdash a : S \quad S \leq T}{\Gamma \vdash a : T}\)
If the reduction semantics of the cast calculus is reasonably defined (see later) then:

**Theorem (Soundness)**

If $\Gamma \vdash a : T$, then $\Gamma \vdash a : T \xrightarrow{\text{compiles}} a'$ and

- either $a'$ reduces to a value of type $T$
- or $a'$ diverges
- or $a'$ fails for a cast on a dynamic type
If the reduction semantics of the cast calculus is reasonably defined (see later) then:

**Theorem (Soundness)**

If \( \Gamma \vdash a : T \), then \( \Gamma \vdash a : T \) \( \xrightarrow{\text{compiles}} a' \) and
- either \( a' \) reduces to a value of type \( T \)
- or \( a' \) diverges
- or \( a' \) fails for a cast on a dynamic type
HM Polymorphism

Syntax:

*Types* \( T \) := \( \text{Int} \mid \text{Bool} \mid T \rightarrow T \mid \alpha \)

*Schemas* \( \sigma \) := \( T \mid \forall \alpha. \sigma \)

*Terms* \( a, b \) := \( x \mid ab \mid \lambda x.a \mid \text{let } x = a \text{ in } b \mid 1 \mid 2 \mid ... \)

Semantics:

\[
(\beta)
(\lambda x.a)b \rightarrow a[b/x]
\]

Typing

\[
\begin{align*}
\Gamma \vdash x : \Gamma(x) & \quad \Gamma, x : S \vdash a : T \\
\Gamma \vdash \lambda x.a : S \rightarrow T & \quad \Gamma \vdash a : S \rightarrow T \\
\Gamma \vdash b : S & \quad \Gamma \vdash ab : T \\
\Gamma \vdash a : \sigma_1 & \quad \Gamma, x : \sigma_1 \vdash b : \sigma_2 \\
\Gamma \vdash \text{let } x = a \text{ in } b : \sigma_2 & \quad \Gamma \vdash a : T \quad \alpha \notin \text{fv}(\Gamma) \\
\Gamma \vdash a : \forall \alpha. T & \quad \Gamma \vdash a : T[S/\alpha]
\end{align*}
\]
HM Polymorphism + Gradual Typing

Syntax:

(types) \( T \ ::= \ \text{Int} \mid \text{Bool} \mid T \to T \mid \alpha \mid ? \)

(schemas) \( \sigma \ ::= T \mid \forall \alpha.\sigma \)

/terms\( a, b \ ::= x \mid ab \mid \lambda x.a \mid \text{let } x = a \text{ in } b \mid 1 \mid 2 \mid ... \)

Semantics:

\[ \frac{\Gamma \vdash a : S \to \text{compiles} \quad S \sqsubseteq T}{\Gamma \vdash a : T \to \text{compiles} \quad a \to \langle T \rangle} \]

Typing

\[ \frac{\Gamma, x : S \vdash a : T}{\Gamma \vdash x : \Gamma(x)} \]

\[ \frac{\Gamma \vdash \lambda x.a : S \to T}{\Gamma \vdash \lambda x.a : S \to T} \]

\[ \frac{\Gamma \vdash ab : T}{\Gamma \vdash b : S} \]

\[ \frac{\Gamma \vdash a : \sigma_1 \quad \Gamma, x : \sigma_1 \vdash b : \sigma_2}{\Gamma \vdash \text{let } x = a \text{ in } b : \sigma_2} \]

\[ \frac{\Gamma \vdash a : T}{\alpha \notin \text{fv}(\Gamma)} \]

\[ \frac{\Gamma \vdash a : \forall \alpha. T}{\Gamma \vdash a : \forall \alpha. T} \]

\[ \frac{\Gamma \vdash a : S}{\text{Materialize} \quad S \sqsubseteq T \quad \Gamma \vdash a : T} \]

\[ \frac{\Gamma \vdash a : T}{\text{Materialize} \quad \Gamma \vdash a : T} \]
HM Polymorphism + Gradual Typing + Subtyping

Syntax:

Types \( T \) ::= \( \text{Int} \mid \text{Bool} \mid T \rightarrow T \mid \alpha \mid ? \)

Schemas \( \sigma \) ::= \( T \mid \forall \alpha.\sigma \)

Terms \( a, b \) ::= \( x \mid ab \mid \lambda x.a \mid \text{let } x = a \text{ in } b \mid 1 \mid 2 \mid ... \)

Semantics:

\[
\begin{align*}
\frac{\Gamma \vdash a : S \text{ compiles} a' \quad S \sqsubseteq T}{\Gamma \vdash a : T \text{ compiles} a'(T)}
\end{align*}
\]

Typing

\[
\begin{align*}
\frac{\Gamma, x : S \vdash a : T}{\Gamma \vdash x : \Gamma(x)} & \quad \frac{\Gamma \vdash \lambda x.a : S \rightarrow T}{\Gamma \vdash a : S \rightarrow T} & \quad \frac{\Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S}{\Gamma \vdash ab : T} \\
\frac{\Gamma \vdash a : \sigma_1 \quad \Gamma, x : \sigma_1 \vdash b : \sigma_2}{\Gamma \vdash \text{let } x = a \text{ in } b : \sigma_2} & \quad \frac{\Gamma \vdash a : T \quad \alpha \notin \text{fv}(\Gamma)}{\Gamma \vdash a : \forall \alpha.T} & \quad \frac{\Gamma \vdash a : \forall \alpha.T}{\Gamma \vdash a : T[S/\alpha]} \\
\frac{\Gamma \vdash a : S \quad S \sqsubseteq T}{\Gamma \vdash a : T} & \quad \frac{\Gamma \vdash a : S \quad S \leq T}{\Gamma \vdash a : T}
\end{align*}
\]
HM Polymorphism + Gradual Typing + Subtyping

Syntax:

**Types**  
\[ T ::= \text{Int} \mid \text{Bool} \mid T \rightarrow T \]

**Schemas**  
\[ \sigma ::= T \mid \forall \alpha.\sigma \]

**Terms**  
\[ a, b ::= x \mid ab \mid \lambda x.a \mid \text{let } x = a \text{ in } b \]

Semantics:

\[
\begin{align*}
\Gamma \vdash a : S & \quad \text{compiles} \quad \rightarrow \quad a' \quad S \trianglerighteq T \\
\Gamma \vdash a : T & \quad \text{compiles} \quad \rightarrow \quad a' \langle T \rangle 
\end{align*}
\]

Typing

\[
\begin{align*}
\Gamma, x : S & \vdash a : T \\
\Gamma & \vdash \lambda x.a : S \rightarrow T \\
\Gamma & \vdash ab : T \\
\Gamma & \vdash a : \sigma_1 \\
\Gamma, x : \sigma_1 & \vdash b : \sigma_2 \\
\Gamma & \vdash \text{let } x = a \text{ in } b : \sigma_2 \\
\Gamma & \vdash a : T \quad \alpha \notin \text{fv}(\Gamma) \\
\Gamma & \vdash a : \forall \alpha. T \\
\Gamma & \vdash a : T[S/\alpha] \\
\Gamma & \vdash a : S \quad S \trianglerighteq T \\
\Gamma & \vdash a : T \quad S \leq T
\end{align*}
\]

Some details are missing: annotations and no inference for gradual types ... but that's it!!

G. Castagna (CNRS)
HM Polymorphism + Gradual Typing + Subtyping

Syntax:

Types $T ::=$ Int $|$ Bool $|$ $T \rightarrow T$

Schemas $\sigma ::= T | \forall \alpha. \sigma$

Terms $a, b ::= x | ab | \lambda x. a | \text{let } x = a \text{ in } b | ...$

Semantics:

$\Gamma \vdash a : S$ \text{ compiles} $\Rightarrow a' \quad S \sqsubseteq T$

Typing

$\Gamma, x : S \vdash a : T$ \quad $\Gamma \vdash a : S \rightarrow T$ \quad $\Gamma \vdash b : S$

$\Gamma \vdash \lambda x. a : S \rightarrow T$ \quad $\Gamma \vdash ab : T$

$\Gamma \vdash a : \sigma_1$ \quad $\Gamma, x : \sigma_1 \vdash b : \sigma_2$ \quad $\Gamma \vdash \alpha \not\in \text{fv}(\Gamma)$ \quad $\Gamma \vdash a : \forall \alpha. T$

$\Gamma \vdash \text{let } x = a \text{ in } b : \sigma_2$ \quad $\Gamma \vdash a : \forall \alpha. T$ \quad $\Gamma \vdash a : T[S/\alpha]$

$\Gamma \vdash a : S$ \quad $S \sqsubseteq T$

$\Gamma \vdash a : T$ \quad $S \sqsubseteq T$

$\Gamma \vdash a : T$
Outline

15 Main ideas

16 Formal system

17 Algorithmic Aspects

18 Criteria for Gradual Typing

19 Implementation issues

20 References
1. Type-checking algorithm

\[
\Gamma \vdash x : \Gamma(x)
\]

\[
\Gamma, x : S \vdash a : T
\]

\[
\Gamma \vdash \lambda x : S. a : S \rightarrow T
\]

\[
\Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S
\]

\[
\Gamma \vdash a b : T
\]

\[
[MATERIALIZE]\]

\[
\Gamma \vdash a : S \quad S \sqsubseteq T
\]

\[
\Gamma \vdash a : T
\]
1. Type-checking algorithm

\[
\frac{\Gamma \vdash x : \Gamma(x)}{\Gamma \vdash x : \Gamma(x)}
\]

\[
\frac{\Gamma \vdash \lambda x : S.a : S \rightarrow T}{\Gamma \vdash \lambda x : S.a : S \rightarrow T}
\]

\[
\frac{\Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S}{\Gamma \vdash ab : T}
\]

\[
\frac{\Gamma, x : S \vdash a : T}{\Gamma \vdash a : T}
\]

\[
\frac{\Gamma \vdash a : S \quad S \sqsubseteq T}{\Gamma \vdash a : T}
\]

It is a sound and complete algorithm:

\[
\Gamma \vdash a : T \iff \Gamma \vdash \Lambda a : S \text{ and } S \sqsubseteq T
\]

Actually this is the good old \[\rightarrow \text{ELIM} \sim \sim \sim \] rule of Siek&Taha (but defined for a sensible relation):

\[
\frac{\Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : U \quad S \sqsubseteq U}{\Gamma \vdash ab : T}
\]

since \(U \sqsubseteq S \iff \exists V. S \sqsubseteq V, U \sqsubseteq V\)
1. Type-checking algorithm

\[
\begin{align*}
\Gamma \vdash \alpha \; x : \Gamma(x) & \quad \Gamma, x : S \vdash \alpha \; a : T \\
\Gamma \vdash \alpha \; \lambda x : S. a : S \rightarrow T & \quad \Gamma \vdash \alpha \; b : U \\
\exists V. S \sqsubseteq V, U \sqsubseteq V & \quad \Gamma \vdash \alpha \; a b : T
\end{align*}
\]
1. Type-checking algorithm

$$\Gamma \vdash a : S \quad \Gamma \vdash b : U$$

$$\Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : U$$

$$\exists V. S \sqsubseteq V, U \sqsubseteq V$$

$$\Gamma \vdash ab : T$$

$$\Gamma \vdash a : T \iff \Gamma \vdash a : S \text{ and } S \sqsubseteq T$$

It is a sound and complete algorithm:
1. Type-checking algorithm

\[\begin{align*}
\Gamma \vdash A x : \Gamma(x) \quad &\quad \Gamma, x : S \vdash A a : T \\
\Gamma \vdash A \lambda x : S. a : S \rightarrow T \quad &\quad \Gamma \vdash A \lambda x : S. a : S \rightarrow T
\end{align*}\]

\[\frac{\Gamma \vdash A a : S \rightarrow T \quad \Gamma \vdash A b : U}{\Gamma \vdash A ab : T} \quad \exists V. S \subseteq V, U \subseteq V\]

It is a sound and complete algorithm:

\[\Gamma \vdash a : T \iff \Gamma \vdash A a : S \text{ and } S \subseteq T\]

Actually this is the good old \([\rightarrow ELIM\subseteq]\) rule of Siek&Taha (but defined for a sensible relation):

\[\frac{\Gamma \vdash A a : S \rightarrow T \quad \Gamma \vdash b : U \quad U \sim S}{\Gamma \vdash A ab : T}\]

since \(U \sim S \iff \exists V. S \subseteq V, U \subseteq V\)
2. Compilation

Thanks to the algorithm every well-typed term is associated to a unique typing derivation: we know *where* to put casts.

\[
\begin{align*}
\Gamma \vdash A : S \rightarrow T \\
\Gamma \vdash A : U \\
\Gamma \vdash A : S \rightarrow T \\
S \sqsubseteq V, U \sqsubseteq V \\
\Gamma \vdash A : V \rightarrow T \\
\Gamma \vdash b : U \\
\Gamma \vdash b : V \\
\Gamma \vdash A : T \\
\end{align*}
\]

Which \(V\) shall we use? Well, obviously:

\[
\min \{W | S \sqsubseteq W, U \sqsubseteq W\}
\]
2. Compilation

Thanks to the algorithm every well-typed term is associated to a unique typing derivation: we know \textit{where} to put casts. Indeed:

\[
\begin{array}{c}
\Gamma \vdash \alpha: S \rightarrow T \\
\Gamma \vdash \beta: U
\end{array}
\Rightarrow
\exists V. S \sqsubseteq V, U \sqsubseteq V
\]

\[\Rightarrow E_{\text{LIM}} \]

\[
\begin{array}{c}
\Gamma \vdash \alpha: S \rightarrow T \\
\Gamma \vdash \beta: U
\end{array}
\Rightarrow
\exists V. S \sqsubseteq V, U \sqsubseteq V
\]
2. Compilation

Thanks to the algorithm every well-typed term is a associated to a unique typing derivation: we know *where* to put casts. Indeed:

\[
\frac{\Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : U}{\exists V. S \sqsubseteq V, U \sqsubseteq V} \quad [\rightarrow \text{ELIM} \sqsubseteq ]
\]

\[
\Gamma \vdash a(b) : T
\]

corresponds to the derivation

\[
\frac{\text{MATER}}{\Gamma \vdash a : S \rightarrow T}
\]

\[
\frac{S \sqsubseteq V \quad T \sqsubseteq T}{\frac{\frac{\text{MATER}}{\Gamma \vdash a : S \rightarrow T}}{\frac{S \rightarrow T \sqsubseteq V \rightarrow T}{\text{ELIM} \rightarrow}}}
\]

\[
\frac{\Gamma \vdash b : U \quad U \sqsubseteq V}{\text{MATER}}
\]

\[
\frac{\frac{\frac{\frac{\text{MATER}}{\Gamma \vdash a : V \rightarrow T}}{\text{ELIM} \rightarrow}}{\Gamma \vdash a : V \rightarrow T}}{\Gamma \vdash a(b) : T}
\]
Thanks to the algorithm every well-typed term is associated to a unique typing derivation: we know *where* to put casts. Indeed:

\[
\begin{align*}
& \Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : U \\
& \exists V. S \sqsubseteq V, U \sqsubseteq V \\
\end{align*}
\]

corresponds to the derivation which tells us where to put cast:

\[
\begin{align*}
\frac{
\begin{align*}
& S \sqsubseteq V \\
& T \sqsubseteq T \\
\end{align*}
\quad
\frac{
\begin{align*}
& \Gamma \vdash a : S \rightarrow T \\
& S \rightarrow T \sqsubseteq V \rightarrow T \\
\end{align*}
\quad
\frac{
\begin{align*}
& \Gamma \vdash b : U \\
& U \sqsubseteq V \\
\end{align*}
\quad
\frac{
\begin{align*}
& \Gamma \vdash a(V \rightarrow T) : V \rightarrow T \\
& \Gamma \vdash b(V) : V \\
\end{align*}
\quad
\frac{
\begin{align*}
& \Gamma \vdash a(V \rightarrow T)(b(V)) : T \\
\end{align*}
\end{align*}
\end{align*}
\]
2. Compilation

Thanks to the algorithm every well-typed term is associated to a unique typing derivation: we know *where* to put casts. Indeed:

\[
\Gamma \vdash \ell a : S \to T \quad \Gamma \vdash \ell b : U \\
\exists V. S \sqsubseteq V, U \sqsubseteq V
\]

corresponds to the derivation which tells us where to put cast:

\[
\text{MATER} \quad \frac{S \subseteq V \quad T \subseteq T}{}
\]

\[
\frac{\text{MATER}}{} \quad \frac{\text{ELIM}}{\Gamma \vdash a : S \to T} \quad \frac{S \to T \sqsubseteq V \to T}{} \quad \frac{\text{MATER}}{} \quad \frac{\text{ELIM}}{\Gamma \vdash b : U} \quad \frac{U \sqsubseteq V}{}
\]

\[
\frac{\text{ELIM}}{} \quad \frac{\Gamma \vdash a \langle V \to T \rangle : V \to T}{\Gamma \vdash a \langle V \to T \rangle (b \langle V \rangle) : T}
\]

Which \(V\) shall we use? well, obviously:

\[
V = \min \{W \mid S \sqsubseteq W, U \sqsubseteq W\}
\]
This yields the following compilation rule:

\[
\Gamma \vdash a : S \rightarrow T \quad \text{compiles} \quad a' \quad \Gamma \vdash b : U \quad \text{compiles} \quad b' \\
\Gamma \vdash \lambda a b : T \quad \text{compiles} \quad a' \langle V \rightarrow T \rangle (b' \langle V \rangle)
\]

\(V = \min \{ W \mid S \sqsubseteq W, U \sqsubseteq W \}\)
2. Compilation

This yields the following compilation rule:

\[
\text{Γ ⊢ } a : S \rightarrow T \quad \text{compiles} \quad a' \\
\text{Γ ⊢ } b : U \quad \text{compiles} \quad b'
\]

\[
\text{Γ ⊢ } ab : T \quad \text{compiles} \quad a'\langle V \rightarrow T\rangle(b'\langle V\rangle)
\]

\[\text{(V = min}_{\subseteq}\{W \mid S \subseteq W, U \subseteq W\})\]

Of course we do not insert the corresponding cast when \(V = S\) or \(V = U\).
This yields the following compilation rule:

\[
\begin{align*}
\Gamma \vdash a : S \to T & \quad \text{compiles} \quad a' \\
\Gamma \vdash b : U & \quad \text{compiles} \quad b' \\
\Gamma \vdash \lambda a \, b : T & \quad \text{compiles} \quad a' \langle V \to T \rangle (b' \langle V \rangle)
\end{align*}
\]

\( V = \min \{ W \mid S \sqsubseteq W, U \sqsubseteq W \} \)

Of course we do not insert the corresponding cast when \( V = S \) or \( V = U \).

Cast insertion different from Siek&Taha: we cast both the function and the argument:

We only use “upcast”, that is cast from less precise to more precise types.

This is formalized by the \([\text{MATERIALIZE}]\) rule for \textit{the language with casts}\ (all the other rules are as before)

\[
\begin{array}{c}
\text{[MATERIALIZE]} \\
\hline
\Gamma \vdash a : S \\
\hline
\Gamma \vdash a \langle T \rangle : T
\end{array}
\]
2. Compilation

This yields the following compilation rule:

\[
\begin{align*}
\Gamma \vdash a & : S \to T & \quad \text{compiles} & \quad a' \\
\Gamma \vdash b & : U & \quad \text{compiles} & \quad b' \\
\Gamma \vdash a \cdot b & : T & \quad \text{compiles} & \quad a' \langle V \to T \rangle (b' \langle V \rangle)
\end{align*}
\]

\( (V = \min \subseteq \{ W \mid S \subseteq W, U \subseteq W \}) \)

Of course we do not insert the corresponding cast when \( V = S \) or \( V = U \).

Cast insertion different from Siek&Taha: we cast both the function and the argument.

We only use “upcast”, that is cast from less precise to more precise types.

This is formalized by the [MATERIALIZE] rule for the language with casts (all the other rules are as before)

\[
\begin{align*}
\Gamma \vdash a & : S \\
S & \subseteq T
\end{align*}
\]

\[
\Gamma \vdash a\langle T \rangle : T
\]

The compilation rules map well-typed terms into well-typed terms: terms are cast to types more precise than their static type.
2. Compilation

This yields the following compilation rule:

\[
\frac{
\Gamma \vdash a : S \to T \quad \Gamma \vdash b : U \quad \text{compiles}\quad V \leftarrow \min \{W \mid S \sqsubseteq W, U \sqsubseteq W\}
}{
\Gamma \vdash ab : T \quad \text{compiles}\quad \Gamma \vdash a'(V \to T)(b'(V))
}
\]

Of course we do not insert the corresponding cast when \( V = S \) or \( V = U \).

Cast insertion different from Siek&Taha: we cast both the function and the argument:

We only use “upcast”, that is cast from less precise to more precise types.

This is formalized by the [MATERIALIZE] rule for the language with casts (all the other rules are as before)

\[
\frac{
\Gamma \vdash a : S \quad S \sqsubseteq T
}{
\Gamma \vdash a\langle T\rangle : T
}
\]

The compilation rules map well-typed terms into well-typed terms: terms are cast to types more precise than their static type.
The cast language

Gradually Typed Language

Syntax:

\[\begin{align*}
\text{Types} & \quad T & \ ::= & \quad \text{Int} & \mid & \text{Bool} & \mid & T \to T & \mid & ? \\
\text{Terms} & \quad a, b & \ ::= & \quad x & \mid & ab & \mid & \lambda x : T. a & \mid & 1 & \mid & 2 & \mid & \ldots
\end{align*}\]

Typing

\[\begin{align*}
\Gamma & \vdash x : \Gamma(x) \\
\Gamma, x : S & \vdash a : T \\
\Gamma & \vdash \lambda x : S. a : S \to T \\
\Gamma & \vdash a : S \to T \\
\Gamma & \vdash b : S \\
\Gamma & \vdash ab : T
\end{align*}\]
The cast language

Gradually Typed Language

Syntax:

\[
\begin{align*}
\text{Types} & \quad T ::= \text{Int} \mid \text{Bool} \mid T \to T \mid ? \\
\text{Terms} & \quad a, b ::= x \mid ab \mid \lambda x : T . a \mid a(T) \mid 1 \mid 2 \mid \ldots
\end{align*}
\]

Typing

\[
\begin{align*}
\Gamma \vdash x : \Gamma(x) & \quad \Gamma, x : S \vdash a : T \\
\Gamma \vdash \lambda x : S . a : S \to T & \quad \Gamma \vdash a : S \to T \quad \Gamma \vdash b : S \\
& \quad \Gamma \vdash ab : T
\end{align*}
\]
The cast language

Gradually Typed Language

Syntax:

Types

\[ T ::= \text{Int} \mid \text{Bool} \mid T \to T \mid ? \]

Terms

\[ a, b ::= x \mid ab \mid \lambda x: T. a \mid a\langle T \rangle \mid 1 \mid 2 \mid ... \]

Typing

\[
\begin{align*}
\Gamma &\vdash x : \Gamma(x) \\
\Gamma &\vdash \lambda x : S. a : S \to T \\
\Gamma &\vdash a : S \to T \quad \Gamma &\vdash b : S \\
\text{[MATERIALIZE]} &\quad \Gamma \vdash a : S \quad S \sqsubseteq T \\
\Gamma &\vdash a\langle T \rangle : T
\end{align*}
\]

Still missing the semantics for casts
The cast language

Gradually Typed Language

Syntax:

Types \( T \) ::= \( \text{Int} \mid \text{Bool} \mid T \rightarrow T \mid ? \)

Terms \( a, b \) ::= \( x \mid ab \mid \lambda x: T.a \mid a \langle T \rangle \mid 1 \mid 2 \mid \ldots \)

Typing

\[
\begin{align*}
\Gamma \vdash x : \Gamma(x) & \quad \Gamma, x : S \vdash a : T \\
\Gamma \vdash \lambda x : S.a : S \rightarrow T & \quad \Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S \\
\Gamma \vdash ab : T & \quad [\text{Materialize}] \quad \Gamma \vdash a : S \quad S \sqsubseteq T \\
& \quad \Gamma \vdash a \langle T \rangle : T \\
\end{align*}
\]

Semantics:

\( (\beta) \quad (\lambda x : T.a)b \longrightarrow a[b/x] \)
The cast language

Gradually Typed Language with Casts

Syntax:

Types

\[ T ::= \text{Int} \mid \text{Bool} \mid T \rightarrow T \mid ? \]

Terms

\[ a, b ::= x \mid ab \mid \lambda x:T.a \mid a<T> \mid 1 \mid 2 \mid \ldots \]

Typing

\[
\begin{align*}
\Gamma \vdash x : \Gamma(x) & \\
\Gamma, x : S \vdash a : T & \\
\Gamma \vdash \lambda x:S.a : S \rightarrow T & \\
\Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S & \\
\Gamma \vdash ab : T & \\
\Gamma \vdash a : S & \\
S \sqsubseteq T & \\
\text{[MATERIALIZE]} & \\
\Gamma \vdash a<T> : T & \\
\end{align*}
\]

Semantics:

\[
(\beta) \quad (\lambda x:T.a)b \rightarrow a[b/x]
\]
The cast language

Gradually Typed Language with Casts

Syntax:

Types \( T \) ::= \( \text{Int} \) | \( \text{Bool} \) | \( T \rightarrow T \) | \( ? \)

Terms \( a, b \) ::= \( x \) | \( ab \) | \( \lambda x:T.a \) | \( a\langle T \rangle \) | 1 | 2 | ...

Typing:

\[
\begin{align*}
\Gamma \vdash x : \Gamma(x) \\
\Gamma, x : S \vdash a : T \\
\Gamma \vdash \lambda x:S.a : S \rightarrow T \\
\Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S \\
\Gamma \vdash ab : T \\
\[\text{[MATERIALIZE]}\] \Gamma \vdash a : S \\
S \sqsubseteq T \\
\Gamma \vdash a\langle T \rangle : T
\end{align*}
\]

Semantics:

\( (\beta) \) \( (\lambda x:T.a)b \rightarrow a[b/x] \)

Still missing the semantics for casts
The cast language

What is the dynamic semantics of casts?

- Easy for non-functional values:
  - From `Int` → 3
  - From `Bool` → Fail

- Not so trivial for functions:
  - Function `foo` is not of type `Int → Int`, nevertheless `(foo ⟨Int → Int⟩)(42)` must not fail: it's applied to an `Int` and returns an `Int`.

  Delay the dynamic check of a type until you get to non-functional values:
  - `(foo ⟨Int → Int⟩)() → (foo(42 ⟨Int⟩))⟨Int⟩`
What is the dynamic semantics of casts?

Easy for non functional values:

\[
\begin{align*}
3\langle\text{Int}\rangle & \rightarrow 3 \\
3\langle\text{Bool}\rangle & \rightarrow \text{Fail}
\end{align*}
\]
The cast language

What is the dynamic semantics of casts?

Easy for non functional values:

\[
\begin{align*}
3\langle\text{Int}\rangle & \rightarrow 3 \\
3\langle\text{Bool}\rangle & \rightarrow \text{Fail}
\end{align*}
\]

If \( T \) is not an arrow type, then for \( a\langle T\rangle \) check whether the result of \( a \) is of type \( T \)
What is the dynamic semantics of casts?

Easy for non functional values:

\[3\langle\text{Int}\rangle \rightarrow 3\]
\[3\langle\text{Bool}\rangle \rightarrow \text{Fail}\]

If \( T \) is not an arrow type, then for \( a\langle T\rangle \) check whether the result of \( a \) is of type \( T \)

Not so trivial for functions:

```javascript
function foo (x : ?) {
    if (x == 42) { return (2*x) } else { true }
}
Consider foo\langle\text{Int}\rightarrow\text{Int}\rangle.
```
The cast language

What is the dynamic semantics of casts?

Easy for non functional values:

\[
\begin{align*}
3 \langle \text{Int} \rangle & \rightarrow 3 \\
3 \langle \text{Bool} \rangle & \rightarrow \text{Fail}
\end{align*}
\]

If $T$ is not an arrow type, then for $a \langle T \rangle$ check whether the result of $a$ is of type $T$

Not so trivial for functions:

```
function foo (x : ?) {
    if (x == 42) { return (2*x)} else { true }
}
```

Consider $\text{foo} \langle \text{Int} \rightarrow \text{Int} \rangle$. Function $\text{foo}$ is not of type $\text{Int} \rightarrow \text{Int}$
The cast language

What is the dynamic semantics of casts?

Easy for non functional values:

\[
3 \langle \text{Int} \rangle \longrightarrow 3 \\
3 \langle \text{Bool} \rangle \longrightarrow \text{Fail}
\]

If \( T \) is not an arrow type, then for \( a \langle T \rangle \) check whether the result of \( a \) is of type \( T \)

Not so trivial for functions:

function foo (x : ?) {
  if (x == 42) { return (2*x)} else { true }
}

Consider \( \text{foo} \langle \text{Int} \rightarrow \text{Int} \rangle \). Function \( \text{foo} \) is not of type \( \text{Int} \rightarrow \text{Int} \), nevertheless \( (\text{foo} \langle \text{Int} \rightarrow \text{Int} \rangle)(42) \) must not fail: it’s applied to an \( \text{Int} \) and returns an \( \text{Int} \).
The cast language

**What is the dynamic semantics of casts?**

Easy for non-functional values:

- $3\langle\text{Int}\rangle \rightarrow 3$
- $3\langle\text{Bool}\rangle \rightarrow \text{Fail}$

If $T$ is not an arrow type, then for $a\langle T\rangle$ check whether the result of $a$ is of type $T$.

Not so trivial for functions:

```javascript
function foo (x : ?) {
  if (x == 42) { return (2*x)} else { true }
}
```

Consider $\text{foo}\langle\text{Int} \rightarrow \text{Int}\rangle$. Function $\text{foo}$ is not $\text{foo}\langle\text{Int} \rightarrow \text{Int}\rangle(\text{exp})$? (exp)?

$\text{(foo}\langle\text{Int} \rightarrow \text{Int}\rangle)(42)$ must not fail: it's applied to an Int and returns an Int.
The cast language

What is the dynamic semantics of casts?

Easy for non functional values:

\[
\begin{align*}
3\langle\text{Int}\rangle & \rightarrow 3 \\
3\langle\text{Bool}\rangle & \rightarrow \text{Fail}
\end{align*}
\]

If \( T \) is not an arrow type, then for \( a\langle T\rangle \) check whether the result of \( a \) is of type \( T \)

Not so trivial for functions:

```javascript
function foo (x : ?) {
    if (x == 42) { return (2*x)} else { true }
}
```

Consider \( \text{foo}\langle\text{Int→Int}\rangle \). Function \( \text{foo} \) is not of type \( \text{Int→Int} \), nevertheless \( (\text{foo}\langle\text{Int→Int}\rangle)(42) \) must not fail: it’s applied to an \( \text{Int} \) and returns an \( \text{Int} \).

Delay the dynamic check of a type until you get to non-functional values
The cast language

What is the dynamic semantics of casts?

Easy for non functional values:

\[
3\langle \text{Int} \rangle \rightarrow 3
\]
\[
3\langle \text{Bool} \rangle \rightarrow \text{Fail}
\]

If \( T \) is not an arrow type, then for \( a\langle T \rangle \) check whether the result of \( a \) is of type \( T \)

Not so trivial for functions:

function foo (x : ?) {
  if (x == 42) { return (2*x)} else { true }
}

Consider \( \text{foo}\langle \text{Int}\rightarrow\text{Int}\rangle \). Function \( \text{foo} \) is not of type \( \text{Int}\rightarrow\text{Int} \), nevertheless \( (\text{foo}\langle \text{Int}\rightarrow\text{Int}\rangle)(42) \) must not fail: it’s applied to an \( \text{Int} \) and returns an \( \text{Int} \).

Delay the dynamic check of a type until you get to non-functional values

\( (\text{foo}\langle \text{Int}\rightarrow\text{Int}\rangle)(\text{exp}) \)
**The cast language**

**What is the dynamic semantics of casts?**

**Easy for non functional values:**

\[
\begin{align*}
3 \langle \text{Int} \rangle & \rightarrow 3 \\
3 \langle \text{Bool} \rangle & \rightarrow \text{Fail}
\end{align*}
\]

If \( T \) is not an arrow type, then for \( a \langle T \rangle \) check whether the result of \( a \) is of type \( T \)

**Not so trivial for functions:**

function foo (x : ?) {
  if (x == 42) { return (2*x)} else { true }
}

Consider \( \text{foo} \langle \text{Int} \rightarrow \text{Int} \rangle \). Function \( \text{foo} \) is not of type \( \text{Int} \rightarrow \text{Int} \), nevertheless \( (\text{foo} \langle \text{Int} \rightarrow \text{Int} \rangle)(42) \) must not fail: it’s applied to an \( \text{Int} \) and returns an \( \text{Int} \).

Delay the dynamic check of a type until you get to non-functional values

\[(\text{foo} \langle \text{Int} \rightarrow \text{Int} \rangle)(42)\]
The cast language

What is the dynamic semantics of casts?

Easy for non functional values:

\[ 3\langle \text{Int} \rangle \longrightarrow 3 \]

\[ 3\langle \text{Bool} \rangle \longrightarrow \text{Fail} \]

If \( T \) is not an arrow type, then for \( a\langle T \rangle \) check whether the result of \( a \) is of type \( T \)

Not so trivial for functions:

```javascript
function foo (x : ?) {
  if (x == 42) { return (2*x)} else { true }
}
```

Consider \( \text{foo}\langle \text{Int} \rightarrow \text{Int} \rangle \). Function \( \text{foo} \) is not of type \( \text{Int} \rightarrow \text{Int} \), nevertheless \( (\text{foo}\langle \text{Int} \rightarrow \text{Int} \rangle)(42) \) must not fail: it’s applied to an \( \text{Int} \) and returns an \( \text{Int} \).

Delay the dynamic check of a type until you get to non-functional values

\[ (\text{foo}\langle \text{Int} \rightarrow \text{Int} \rangle)(42) \longrightarrow (\text{foo}(42\langle \text{Int} \rangle))\langle \text{Int} \rangle \]
The cast language

Syntax:

**Types**

\[ T ::= \text{Int} | \text{Bool} | T \rightarrow T | ? \]

**Terms**

\[ a, b ::= x | ab | \lambda x:T.a | a\langle T \rangle | 1 | 2 | ... \]

**Values**

\[ v ::= \lambda x:T.a | 1 | 2 | ... \]

Typing

\[ \Gamma \vdash x : S \Gamma(x) \]

\[ \Gamma \vdash x : \Gamma(x) \]

\[ \Gamma \vdash \lambda x:S.a : S \rightarrow T \]

\[ \Gamma \vdash a : S \rightarrow T \Gamma \vdash b : S \]

\[ \Gamma \vdash ab : T \]

\[ \Gamma \vdash a : S \Gamma \vdash a\langle T \rangle : T \]

[MATERIALIZE] \[ \Gamma \vdash a \hspace{0.5cm} S \subseteq T \]

\[ \Gamma \vdash a\langle T \rangle : T \]

Semantics:

\[ (\lambda x:T.a)v \rightarrow a[v/x] \]

\[ v\langle T \rangle \rightarrow v \]

\[ v\langle T \rangle \rightarrow \text{Fail} \]

\[ (v_1\langle S \rightarrow T \rangle)v_2 \rightarrow (v_1(v_2\langle S \rangle))\langle T \rangle \]

if \( T \neq S_1 \rightarrow S_2 \) and \( \Gamma \vdash v : T \)

if \( T \neq S_1 \rightarrow S_2 \) and \( \nabla \vdash v : T \)
The cast language is sound:

**Theorem (Soundness)**

For every term $a$ of the cast language, if $\Gamma \vdash a : T$, then
- either $a$ reduces to a value of type $T$
- or $a$ diverges
- or $a$ reduces to $\text{Fail}$

[no stuck term]

What are the consequences of this theorem on our initial language? How does it fit our framework? Let me first add a further bit
Tracking errors

The message Fail is not very useful for debugging
Tracking errors

The message Fail is not very useful for debugging

We can modify compilation to track the origin of failures:

\[
\text{[MATERIALIZE] } \frac{\Gamma \vdash a : S \text{ compiles } a' \quad S \sqsubseteq T}{\Gamma \vdash a : T \text{ compiles } a'\langle T\rangle^\ell}
\]

where \( \ell \) is a pointer to the source code of \( a \)
Tracking errors

The message Fail is not very useful for debugging

We can modify compilation to track the origine of failures:

\[
\frac{\Gamma \vdash a : S \text{ compiles } a' \quad S \sqsubseteq T}{\Gamma \vdash a : T \text{ compiles } a'(T)\ell}
\]

where \(\ell\) is a pointer to the source code of \(a\)

Then it suffices to change the semantics of the cast language to return this pointer:

Semantics:

\[
(\lambda x : T. a) v \rightarrow a[v/x]
\]

\[
v(T)\ell \rightarrow v
\]

\[
v(T)\ell \rightarrow \text{blame } \ell
\]

\[
(v_1(S \rightarrow T)\ell) v_2 \rightarrow (v_1(v_2(S)\ell)(T)\ell
\]

if \(T \neq S_1 \rightarrow S_2\) and \(\vdash v : T\)

if \(T \neq S_1 \rightarrow S_2\) and \(\nvdash v : T\)
Outline

15 Main ideas

16 Formal system

17 Algorithmic Aspects

18 Criteria for Gradual Typing

19 Implementation issues

20 References
Every expression must only result in values whose type agrees with the static type of the expression.
Every expression must only result in values whose type agrees with the static type of the expression.

**Theorem (Soundness)**

If $\Gamma \vdash a : T$, then $\Gamma \vdash a : T \xrightarrow{\text{compiles}} a'$ and

- either $a'$ reduces to a value of type $T$
- or $a'$ diverges
- or $a'$ fails for a cast on a dynamic type
Every expression must only result in values whose type agrees with the static type of the expression.

**Theorem (Soundness)**

If $\Gamma \vdash a : T$, then $\Gamma \vdash a : T \xrightarrow{\text{compiles}} a'$ and
- either $a'$ reduces to a value of type $T$
- or $a'$ diverges
- or $a'$ fails for a cast on a dynamic type

A Corollary of the soundness of the cast calculus and of the following lemma of type preservation.

**Lemma.** If $\Gamma \vdash a : T$ then then $\Gamma \vdash a : T \xrightarrow{\text{compiles}} a'$ and $\Gamma \vdash a' : S \subseteq T$
Criterion: Blame Tracking

When a runtime type error occurs, it is never the fault of a statically typed region of code.
When a runtime type error occurs, it is never the fault of a statically typed region of code.

**Theorem (Blame Theorem)**

Let $C[a]$ be a program such that $\omega$ does not occur in $a$. If $\Gamma \vdash C[a] : T \xrightarrow{\text{compiles}} b$ and $b \xrightarrow{\text{blame}} l$, then $l \in C[]$ and $l \not\in a$. 
Using less precise types must not change the outcome of type checking or of running a program.
Using less precise types must not change the outcome of type checking or of running a program.

An expression $a$ is *less precise* than $b$, written $a \sqsubseteq b$, if $a$ is $b$ but with less precise annotations.

**Note:** a dynamically typed version of $a$ is where all annotations are $\square$: it is a minimal element in the precision lattice.
Criterion: Gradual Guarantee

Using less precise types must not change the outcome of type checking or of running a program.

An expression $a$ is less precise than $b$, written $a \sqsubseteq b$, if $a$ is $b$ but with less precise annotations.

Note: a dynamically typed version of $a$ is where all annotations are $?$: it is a minimal element in the precision lattice.

Theorem (Gradual Guarantee)

If $\Gamma \vdash a : T \xrightarrow{\text{compiles}} a'$ and $b \sqsubseteq a$, then:

- $\Gamma \vdash b : T' \xrightarrow{\text{compiles}} b'$ and $T' \sqsubseteq T$
- If $a' \rightarrow v$, then $b' \rightarrow v'$ and $v' \sqsubseteq v$. 

Outline

15 Main ideas
16 Formal system
17 Algorithmic Aspects
18 Criteria for Gradual Typing
19 Implementation issues
20 References
A hint to efficient implementation

A gradually typed tail-recursive function:

```ocaml
let rec odd : Int -> ? = fun n ->
  if n = 0 then false
else (even (n-1))

and even : Int -> Bool = fun n ->
  if n = 0 then true
else (odd (n-1))
```

It produces accumulation of casts:

```
odd 5
→ (even 4)\<?
→ (odd 3)<Bool>\<?
→ (even 2)<Bool>\<?
→ (odd 1)<Bool>\<?
→ (even 0)<Bool>\<?
```

Solution:

Specific implementation of tail-recursion combine with cast compression via intersection types:

\[ E \langle \tau \rangle \langle \tau' \rangle \text{ can be “compressed” to } E \langle \tau \land \tau' \rangle. \]
A hint to efficient implementation

A gradually typed tail-recursive function: In Siek&Taha it is compiled into:

```ml
let rec odd : Int -> ? = fun n ->
    if n = 0 then false<?>
    else (even (n-1))<?>

and even : Int -> Bool = fun n ->
    if n = 0 then true
    else (odd (n-1))<Bool>
```

Solution: specific implementation of tail-recursion combine with cast compression via intersection types:

\[ E\langle \tau \rangle\langle \tau' \rangle \text{ can be } E\langle \tau \land \tau' \rangle. \]
A hint to efficient implementation

A gradually typed tail-recursive function:

```haskell
let rec odd : Int -> ? = fun n ->
  if n = 0 then false
  else (even (n-1))

and even : Int -> Bool = fun n ->
  if n = 0 then true
  else (odd (n-1))
```

It produces accumulation of casts:

```
odd 5  →  (even 4)
    →  (odd 3)<Bool>
    →  (even 2)<Bool><Bool>
    →  (odd 1)<Bool><Bool><Bool>
    →  (even 0)<Bool><Bool><Bool><Bool>
```
A hint to efficient implementation

A gradually typed tail-recursive function:

```plaintext
let rec odd : Int -> ? = fun n ->
  if n = 0 then false<?>
  else (even (n-1))<?>

and even : Int -> Bool = fun n ->
  if n = 0 then true
  else (odd (n-1))<Bool>
```

It produces accumulation of casts:

- `odd 5` → `(even 4)`
- → `(odd 3)`
- → `(even 2)`
- → `(odd 1)`
- → `(even 0)`

**Solution:** specific implementation of tail-recursion combine with cast compression via intersection types:

\[ E\langle\tau\rangle\langle\tau'\rangle \text{ can be “compressed” to } E\langle\tau \land \tau'\rangle. \]
### Syntax:

**Types**
\[
T ::= \text{Int} \mid \text{Bool} \mid T \rightarrow T \mid \alpha \mid ?
\]

**Schemas**
\[
\sigma ::= T \mid \forall \alpha.\sigma
\]

**Terms**
\[
a, b ::= x \mid ab \mid \lambda x . a \mid \text{let } x = a \text{ in } b \mid 1 \mid 2 \mid ...
\]

### Semantics:

\[
\frac{\text{[MATERIALIZE}_{\text{COMPIL}}]}{\Gamma \vdash a : S \quad \text{compiles} \quad a' \quad S \sqsubseteq T} \quad \frac{\Gamma \vdash a : T \quad \text{compiles} \quad a' \langle T \rangle}
\]

### Typing

\[
\frac{\Gamma \vdash x : \Gamma(x)}{\Gamma \vdash a : T} \quad \frac{\Gamma, x : S \vdash a : T}{\Gamma \vdash \lambda x . a : S \rightarrow T} \quad \frac{\Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S}{\Gamma \vdash ab : T}
\]

\[
\frac{\Gamma \vdash a : \sigma_1 \quad \Gamma, x : \sigma_1 \vdash b : \sigma_2}{\Gamma \vdash \text{let } x = a \text{ in } b : \sigma_2} \quad \frac{\Gamma \vdash a : T \quad \alpha \not\in \text{fv}(\Gamma)}{\Gamma \vdash a : \forall \alpha . T} \quad \frac{\Gamma \vdash a : \forall \alpha . T}{\Gamma \vdash a : T[S/\alpha]}
\]

\[
\frac{\Gamma \vdash a : S \quad S \sqsubseteq T}{\Gamma \vdash a : T} \quad \text{[MATERIALIZE]}
\]
Syntax:

Types \( T \) ::=
\[ \text{Int} \mid \text{Bool} \mid T \rightarrow T \mid \alpha \mid ? \]

Schemas \( \sigma \) ::=
\[ T \mid \forall \alpha.\sigma \]

Terms \( a, b \) ::=
\[ x \mid ab \mid \lambda x.a \mid \text{let } x = a \text{ in } b \mid 1 \mid 2 \mid \ldots \]

Semantics:

\[
\begin{align*}
\text{[MATERIALIZE\textsubscript{COMPIL}]} & \quad \Gamma \vdash a : S \quad \text{compiles} \quad a' \quad S \sqsubseteq T \\
\Gamma \vdash a : T \quad \text{compiles} \quad a'\langle T \rangle
\end{align*}
\]

Typing

\[
\begin{align*}
\Gamma \vdash x : \Gamma(x) & \quad \Gamma, x : S \vdash a : T \\
\Gamma \vdash \lambda x.a : S \rightarrow T & \quad \Gamma \vdash a : S \rightarrow T \quad \Gamma \vdash b : S \\
\Gamma \vdash ab : T & \\
\Gamma \vdash a : \sigma_1 \quad \Gamma, x : \sigma_1 \vdash b : \sigma_2 & \quad \Gamma \vdash a : T \quad \alpha \not\in \text{fv}(\Gamma) \\
\Gamma \vdash \text{let } x = a \text{ in } b : \sigma_2 & \quad \Gamma \vdash a : \forall \alpha.\mathcal{T} \\
\Gamma \vdash a : \forall \alpha.\mathcal{T} & \quad \Gamma \vdash a : T[S/\alpha]
\end{align*}
\]

\[
\begin{align*}
\text{[MATERIALIZE]} & \quad \Gamma \vdash a : S \quad S \sqsubseteq T \\
\Gamma \vdash a : T & \quad \text{[SUBSUM]} \quad \Gamma \vdash a : S \quad S \leq T
\end{align*}
\]
HM Polymorphism + Gradual Typing + Subtyping

Syntax:

Types $T ::= \text{Int} \mid \text{Bool} \mid T \rightarrow T$

Schemas $\sigma ::= T \mid \forall \alpha.\sigma$

Terms $a, b ::= x \mid ab \mid \lambda x.a \mid \text{let } x = a \text{ in } b$

Semantics:

\[
\frac{\Gamma \vdash a : S \quad S \sqsubseteq T}{\Gamma \vdash a : T}
\]

Typing

\[
\frac{\Gamma, x : S \vdash a : T}{\Gamma \vdash \lambda x.a : S \rightarrow T}
\]

Some details are missing: annotations and no inference for gradual types ... but that's it!!

\[
\frac{\Gamma \vdash a : \sigma_1 \quad \Gamma, x : \sigma_1 \vdash b : \sigma_2}{\Gamma \vdash \text{let } x = a \text{ in } b : \sigma_2}
\]

\[
\frac{\Gamma \vdash a : T \quad \alpha \notin \text{fv}(\Gamma)}{\Gamma \vdash a : \forall \alpha.T}
\]

\[
\frac{\Gamma \vdash a : \forall \alpha.T}{\Gamma \vdash a : T[S/\alpha]}
\]

\[
\frac{\Gamma \vdash a : S \quad S \sqsubseteq T}{\Gamma \vdash a : T}
\]

\[
\frac{\Gamma \vdash a : S \quad S \leq T}{\Gamma \vdash a : T}
\]
HM Polymorphism + Gradual Typing + Subtyping

Syntax:

Types \( T \) ::= Int \mid Bool \mid T \to T \mid \alpha \mid \text{???}

Schemas \( \sigma \) ::= \( T \mid \forall \alpha.\sigma \)

Terms \( a, b \) ::= \( x \mid ab \mid \lambda x.a \mid \text{let } x = a \text{ in } b \mid \ldots \)

Semantics:

That's all, but how do I implement it?!!?

Typing

\[ \Gamma \vdash a : \sigma_1 \quad \Gamma, x : \sigma_1 \vdash b : \sigma_2 \]
\[ \Gamma \vdash \text{let } x = a \text{ in } b : \sigma_2 \]

\[ \Gamma \vdash a : T \quad \alpha \not\in \text{fv}(\Gamma) \]
\[ \Gamma \vdash a : \forall \alpha. T \]
\[ \Gamma \vdash a : T[S/\alpha] \]

\[ \Gamma \vdash a : S \quad S \sqsubseteq T \]
\[ \Gamma \vdash a : T \]

\[ \Gamma \vdash a : T \]

\[ \Gamma \vdash a : S \quad S \leq T \]

\[ \Gamma \vdash a : T \]
The missing details

Syntax:

**StaticTypes**

\[ T ::= \text{Int} \mid \text{Bool} \mid T \rightarrow T \mid \alpha \]

**GradualTypes**

\[ \tau ::= \text{Int} \mid \text{Bool} \mid \tau \rightarrow \tau \mid \alpha \mid ? \]

**Schemas**

\[ \sigma ::= T \mid \forall \alpha.\sigma \]

**Terms**

\[ a, b ::= x \mid ab \mid \lambda x.a \mid \lambda x: \tau.a \mid \text{let } x = a \text{ in } b \mid 1 \mid 2 \]

Typing

\[
\begin{align*}
\Gamma \vdash a : \tau' \rightarrow \tau & \quad \Gamma \vdash b : \tau' \\
\Gamma \vdash x : \Gamma(x) & \\
\Gamma \vdash ab : \tau \\
\Gamma, x : \tau \vdash a : \tau' & \\
\Gamma \vdash \lambda x: \tau.a : \tau' \rightarrow \tau' & \\
\Gamma, x : S \vdash a : \tau & \\
\Gamma \vdash \lambda x.a : S \rightarrow \tau \\
\Gamma \vdash a : \sigma_1 & \\
\Gamma, x : \sigma_1 \vdash b : \sigma_2 & \\
\Gamma \vdash \text{let } x = a \text{ in } b : \sigma_2 \\
\Gamma \vdash a : \tau & \quad \alpha \not\in \text{fv}(\Gamma) \\
\Gamma \vdash a : \forall \alpha.\tau & \\
\Gamma \vdash a : \tau'[\tau'/\alpha] \\
\end{align*}
\]

**Materialize**

\[
\begin{align*}
\Gamma \vdash a : \tau' \quad \tau' \subseteq \tau & \quad \Gamma \vdash a : \tau \\
\end{align*}
\]

**Subsum**

\[
\begin{align*}
\Gamma \vdash a : \tau' \quad \tau' \leq \tau & \quad \Gamma \vdash a : \tau \\
\end{align*}
\]
Part 1: Without subtyping

We generate sets $D$ of *type constraints*

\[
D ::= \emptyset \mid (t_1 \preceq t_2) \cup D \mid (\tau \sqsubseteq \alpha) \cup D
\]

Then we find a type substitution $\theta$ that *solves* $D$ that is

- for all $(t_1 \preceq t_2)$ we have $t_1 \theta = t_2 \theta$
- for all $(\tau \sqsubseteq \alpha)$ we have $\tau \theta \sqsubseteq \alpha \theta$ and $\tau \theta$ is a static type
Constraint generation

We do not directly generate type constraint. We first \emph{generate structured constraints} of the form\footnote{Let constraints are omitted for the sake of simplicity}:

\[
C ::= (t \leq t) \mid (\tau \sqsubseteq \alpha) \mid (x \sqsubseteq \alpha) \mid \texttt{def } x : \tau \texttt{ in } C \mid \exists \alpha. C \mid C \land C
\]
Constraint generation

We do not directly generate *type constraint*. We first *generate structured constraints* of the form\(^1\):

\[
C ::= (t \leq t) \mid (\tau \sqsubseteq \alpha) \mid (x \sqsubseteq \alpha) \mid \text{def } x : \tau \text{ in } C \mid \exists \bar{\alpha}. C \mid C \land C
\]

\[
\langle \langle x : t \rangle \rangle = \exists \alpha. (x \sqsubseteq \alpha) \land (\alpha \leq t)
\]

\[
\langle \langle \lambda x. e : t \rangle \rangle = \exists \alpha_1, \alpha_2. (\text{def } x : \alpha_1 \text{ in } \langle \langle e : \alpha_2 \rangle \rangle) \land (\alpha_1 \sqsubseteq \alpha_1) \land (\alpha_1 \rightarrow \alpha_2 \leq t)
\]

\[
\langle \langle \lambda x : \tau. e : t \rangle \rangle = \exists \alpha_1, \alpha_2. (\text{def } x : \tau \text{ in } \langle \langle e : \alpha_2 \rangle \rangle) \land (\tau \sqsubseteq \alpha_1) \land (\alpha_1 \rightarrow \alpha_2 \leq t)
\]

\[
\langle \langle e_1 e_2 : t \rangle \rangle = \exists \alpha. \langle \langle e_1 : \alpha \rightarrow t \rangle \rangle \land \langle \langle e_2 : \alpha \rangle \rangle
\]

\(^1\)Let constraints are omitted for the sake of simplicity
Constraint generation

We do not directly generate type constraint. We first generate structured constraints of the form\(^1\):

\[
C ::= (t \dot{\leq} t) \mid (\tau \subseteq \alpha) \mid (x \dot{\subseteq} \alpha) \mid \text{def } x : \tau \text{ in } C \mid \exists \alpha. C \mid C \land C
\]

\[
\langle x : t \rangle = \exists \alpha. (x \dot{\subseteq} \alpha) \land (\alpha \dot{\leq} t)
\]
\[
\langle (\lambda x . e) : t \rangle = \exists \alpha_1, \alpha_2. (\text{def } x : \alpha_1 \text{ in } \langle e : \alpha_2 \rangle) \land (\alpha_1 \subseteq \alpha_1) \land (\alpha_1 \rightarrow \alpha_2 \dot{\leq} t)
\]
\[
(\lambda x : \tau . e) : t = \exists \alpha_1, \alpha_2. (\text{def } x : \tau \text{ in } \langle e : \alpha_2 \rangle) \land (\tau \subseteq \alpha_1) \land (\alpha_1 \rightarrow \alpha_2 \dot{\leq} t)
\]
\[
\langle e_1 e_2 : t \rangle = \exists \alpha. \langle e_1 : \alpha \rightarrow t \rangle \land \langle e_2 : \alpha \rangle
\]

Note that \(\langle (\lambda x : ? . x) : \text{Int } \rightarrow \text{Int} \rangle\) can be solved, whereas \(\langle (\lambda x . x) : ? \rightarrow ? \rangle\) cannot.

\(^1\)Let constraints are omitted for the sake of simplicity
Rewriting constraints

We then *rewrite the structured constraints* to obtain a set $D$ of *type constraints*:
We then *rewrite the structured constraints* to obtain a set $D$ of *type constraints*:

\[
\Gamma \vdash (x \sqsubseteq \alpha) \leadsto \{ \tau[\vec{\alpha} := \vec{\beta}] \sqsubseteq \alpha \}
\]

$\Gamma(x) = \forall \vec{\alpha}. \tau$

$\vec{\beta}$ FRESH
We then *rewrite the structured constraints* to obtain a set $D$ of *type constraints*:

\[
\Gamma \vdash (x \sqsubseteq \alpha) \leadsto \{ \tau[\vec{\alpha} := \vec{\beta}] \sqsubseteq \alpha \} \\
\Gamma(x) = \forall \vec{\alpha}.\tau \\
\vec{\beta} \text{ FRESH}
\]

\[
(\Gamma, x : \tau) \vdash C \leadsto D \\
\Gamma \vdash \text{def } x : \tau \text{ in } C \leadsto D
\]

\[
\Gamma \vdash C_1 \leadsto D_1 \quad \Gamma \vdash C_2 \leadsto D_2 \\
\Gamma \vdash C_1 \land C_2 \leadsto D_1 \cup D_2
\]
Solving constraints

Everything is finally solved using **standard unification**: (1) we *replace every occurrence* of ? in materialization constraints by a *distinct fresh type variable*; (2) we *unify*; (3) we replace every *residual* fresh type variable *back* to ?.
Solving constraints

Everything is finally solved using **standard unification**:

1. we *replace every occurrence* of ? in materialization constraints by a *distinct fresh type variable*;
2. we *unify*;
3. we replace every *residual* fresh type variable *back* to ?.

For example, the constraint

\[ ? \rightarrow ? \rightarrow ? \subseteq \text{Bool} \rightarrow \alpha \]
Solving constraints

Everything is finally solved using standard unification:

1. we *replace every occurrence* of ? in materialization constraints by a *distinct fresh type variable*;
2. we *unify*;
3. we replace every *residual* fresh type variable *back* to ?.

For example, the constraint

\[ ? \rightarrow ? \rightarrow ? \sqsubseteq \text{Bool} \rightarrow \alpha \]

will become

\[ X_1 \rightarrow X_2 \rightarrow X_3 \sqsubseteq \text{Bool} \rightarrow \alpha \]
Solving constraints

Everything is finally solved using **standard unification**:

1. we *replace every occurrence* of $?$ in materialization constraints by a *distinct fresh type variable*;
2. we *unify*;
3. we replace every *residual* fresh type variable *back* to $?$. 

For example, the constraint

$$?? \rightarrow ?? \rightarrow ?? \sqsubseteq \text{Bool} \rightarrow \alpha$$

will become

$$X_1 \rightarrow X_2 \rightarrow X_3 \sqsubseteq \text{Bool} \rightarrow \alpha$$

and solving it will return the unifier

$$\theta : X_1 \mapsto \text{Bool}; X_2 \mapsto \beta; X_3 \mapsto \gamma; \alpha \mapsto (\beta \rightarrow \gamma)$$
Solving constraints

Everything is finally solved using **standard unification**:
1. we replace *every occurrence* of ? in materialization constraints by a *distinct fresh type variable*;
2. we **unify**;
3. we replace every *residual* fresh type variable back to ?.

For example, the constraint

\[
? \rightarrow ? \rightarrow ? \sqsubseteq \text{Bool} \rightarrow \alpha
\]

will become

\[
X_1 \rightarrow X_2 \rightarrow X_3 \sqsubseteq \text{Bool} \rightarrow \alpha
\]

and solving it will return the unifier

\[
\theta : X_1 \mapsto \text{Bool}; X_2 \mapsto \beta; X_3 \mapsto \gamma; \alpha \mapsto (\beta \rightarrow \gamma)
\]

The application of \( e_1 : (\text{Bool} \rightarrow \alpha) \rightarrow \alpha \) to \( e_2 : ? \rightarrow ? \rightarrow ? \) has thus type ? \rightarrow ?
To summarize, given an expression $e$, and a constraint derivation $\mathcal{D}$ of $\Gamma \vdash \langle\langle e : t \rangle\rangle \rightsquigarrow D$, we can compute a unifier $\theta$ satisfying $\mathcal{D}$. This derivation and the associated unifier can be used to compile $e$ in a straightforward way: to every materialization constraint introduced in $\mathcal{D}$ corresponds a cast. For instance if $\mathcal{D} = \Gamma \vdash \langle\langle x : t \rangle\rangle \rightsquigarrow \{ (\tau \triangleright \alpha), (\alpha \triangleright t) \}$ and $\theta$ is a solution for $\{ (\tau \triangleright \alpha), (\alpha \triangleright t) \}$ then $\mathcal{D}; \theta \vdash x \triangleright x[\alpha\theta]$.

Inference (and compilation) for this system is sound, type-preserving and complete w.r.t. the declarative system.
Compilation and Results

To summarize, given an expression \( e \), and a constraint derivation \( D \) of \( \Gamma \vdash \langle\langle e : t \rangle\rangle \leadsto D \), we can compute a unifier \( \theta \) satisfying \( D \).

This derivation and the associated unifier can be used to compile \( e \) in a straightforward way: to every materialization constraint introduced in \( D \) corresponds a cast.

For instance if \( D = \Gamma; \vdash \langle\langle x : t \rangle\rangle \leadsto \{(\tau \sqsubseteq \alpha), (\alpha \leq t)\} \) and \( \theta \) is a solution for \( \{(\tau \sqsubseteq \alpha), (\alpha \leq t)\} \) then...
To summarize, given an expression \( e \), and a constraint derivation \( \mathcal{D} \) of \( \Gamma \vdash \langle\langle e : t \rangle\rangle \leadsto D \), we can compute a unifier \( \theta \) satisfying \( \mathcal{D} \).

This derivation and the associated unifier can be used to compile \( e \) in a straightforward way: to every materialization constraint introduced in \( \mathcal{D} \) corresponds a cast. For instance if \( \mathcal{D} = \Gamma; \vdash \langle\langle x : t \rangle\rangle \leadsto \{ (\tau \sqsubseteq \alpha), (\alpha \leq t) \} \) and \( \theta \) is a solution for \( \{ (\tau \sqsubseteq \alpha), (\alpha \leq t) \} \) then

\[
\mathcal{D}; \theta \vdash x \rightarrow x\langle\alpha\theta\rangle
\]

Inference (and compilation) for this system is sound, type-preserving and complete w.r.t. the declarative system.
Part 2: Adding subtyping

We saw that, declaratively, *adding subtyping* is just a matter of adding *one subsumption rule*. 
Part 2: Adding subtyping

We saw that, declaratively, *adding subtyping* is just a matter of adding *one subsumption rule*.

*Constraint generation* is also unchanged, unification constraints just become *subtyping constraints*. 
Part 2: Adding subtyping

We saw that, declaratively, adding subtyping is just a matter of adding one subsumption rule.

*Constraint generation* is also unchanged, unification constraints just become subtyping constraints.

However, to solve constraints such as $\{(\alpha \leq t_1), (\alpha \leq t_2)\}$ we have to compute greatest lower bounds.
Part 2: Adding subtyping

We saw that, declaratively, adding subtyping is just a matter of adding one subsumption rule.

Constraint generation is also unchanged, unification constraints just become subtyping constraints.

However, to solve constraints such as \{ (\alpha \leq t_1), (\alpha \leq t_2) \} we have to compute greatest lower bounds.

For example,

\[ \text{fun } x \to \text{if (fst x) then (1 + snd x) else x} \]

should be of type \((\text{Bool} \times \text{Int}) \rightarrow (\text{Int} \mid (\text{Bool} \times \text{Int}))\)
Part 3: Adding Set-Theoretic Types

The types become:

\[
\text{StaticTypes} \quad T ::= \text{Int} \mid \text{Bool} \mid T \rightarrow T \mid T \lor T \mid \neg T \mid \text{Any} \mid \alpha \\
\text{GradualTypes} \quad \tau ::= \text{Int} \mid \text{Bool} \mid \tau \rightarrow \tau \mid \alpha \mid \text{??}
\]

\[
\text{Schemas} \quad \sigma ::= T \mid \forall \alpha.\sigma
\]

Constraints are \textit{unchanged}. However, the inference algorithm is now based on the \textit{tallying algorithm} of Castagna et al. [2015], rather than unification (but the principle is the same).

\[
\{(\alpha \preceq t_1), (\alpha \preceq t_2)\} \leadsto \{(\alpha \preceq t_1 \land t_2)\}
\]
The types become:

**StaticTypes**  
\[ T ::= \text{Int} \mid \text{Bool} \mid T \rightarrow T \mid T \lor T \mid \neg T \mid \text{Any} \mid \alpha \]

**GradualTypes**  
\[ \tau ::= \text{Int} \mid \text{Bool} \mid \tau \rightarrow \tau \mid \alpha \mid ?? \]

**Schemas**  
\[ \sigma ::= T \mid \forall \alpha. \sigma \]

Constraints are *unchanged*. However, the inference algorithm is now based on the *tallying algorithm* of Castagna et al. [2015], rather than unification (but the principle is the same).

\[
\{(\alpha \preceq t_1), (\alpha \preceq t_2)\} \leadsto \{ (\alpha \preceq t_1 \land t_2) \}
\]

*Soundness still holds* for the inference algorithm, but *completeness no longer holds*. 
Outline

15 Main ideas

16 Formal system

17 Algorithmic Aspects

18 Criteria for Gradual Typing

19 Implementation issues

20 References
To go further

Some starting points:

- **Objects:** Siek & Taha (ECOOP 2007)
- **Type inference:** Siek & Vachharajani (DLS 2008), Garcia & Cimini (POPL 2015) [both superseded by Castagna & al (POPL 2019)]
- **Occurrence Typing:** Tobin-Hochstadt & Felleisen (POPL 2008)
- **Foundational approach:** Garcia & Clark & Tanter (POPL 2016)
- **Gradual Guarantees:** Siek & Vitousek & Cimini & Boyland (SNAPL 2015)
- **Second order parametric polymorphism:** Igarashi et al. (ICFP 2017), Xie & Bi & Oliveira (ESOP 2018)
- **Union and intersection types:** Castagna & Lanvin (ICFP 2017)
- **Implementation aspects:** Takikawa et al. (POPL 2016), Bauman et al. (OOPSLA 2017), Kuhlenschmidt et al. (PLDI 2019), Castagna & Duboc & Lanvin & Siek (IFL 2019)
- **Type inference, subtyping, union and intersection types:** Castagna & Lanvin & Petrucciani & Siek (POPL 2019) **The full monty!**