Design Principles of Programming Languages

编程语言的设计原理

Haiyan Zhao, Di Wang

赵海燕，王迪

Peking University, Spring Term 2024

Type-Level Computation

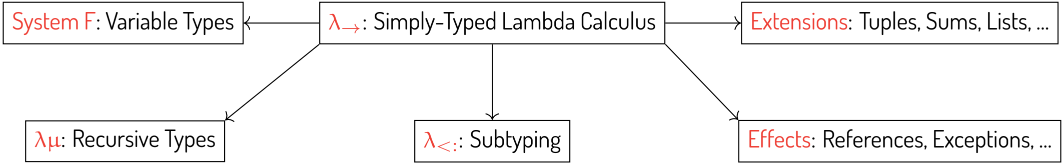
类型层计算

We Have Studied ...

Principle

The uses of type systems go beyond detecting errors.

- Type systems offer support for **abstraction**, **safety**, **efficiency**, ...
- Language design goes **hand-in-hand** with type-system design.



Observation

Different **combinations** lead to different languages.

- System F + $\lambda\mu$ supports polymorphic recursive types.
- System F + $\lambda_{<:}$ supports bounded quantification (see Chap. 26).

The Essence of λ

Principle (Computation)

λ-abstraction is **THE** mechanism of defining computation.

- In $\lambda_{\to}$, $\lambda x{:}T.\ t$ abstracts **terms** out of **terms**.
- In System F, $\lambda X.\ t$ abstracts **terms** out of **types**.

Principle (Characterization of Computation)

Typing is **THE** mechanism of characterizing computation.

- Syntactically: **types** characterize **terms**.
- Semantically: a **type** denotes a set of **terms** that evaluates to particular values.

Question

Can we introduce computation to the type level?
How to characterize such type-level computation?

Type Operators

Remark

We have seen **parametric** type definitions:

$\mathtt{Pair}_{\mathtt{T1,T2}} = \forall \mathtt{X}.\ (\mathtt{T1} \to \mathtt{T2} \to \mathtt{X}) \to \mathtt{X};$

$\mathtt{Sum}_{\mathtt{T1,T2}} = \forall \mathtt{X}.\ (\mathtt{T1} \to \mathtt{X}) \to (\mathtt{T2} \to \mathtt{X}) \to \mathtt{X};$

$\mathtt{List}_{\mathtt{T}} = \forall \mathtt{x}.\ (\mathtt{T} \to \mathtt{X} \to \mathtt{X}) \to \mathtt{X} \to \mathtt{X};$

Observation

Pair, Sum, and List behave like **type-level functions**!

$\mathtt{Pair} = \lambda \mathtt{T1}.\ \lambda \mathtt{T2}.\ (\forall \mathtt{X}.\ (\mathtt{T1} \to \mathtt{T2} \to \mathtt{X}) \to \mathtt{X});$

$\mathtt{Sum} = \lambda \mathtt{T1}.\ \lambda \mathtt{T2}.\ (\forall \mathtt{X}.\ (\mathtt{T1} \to \mathtt{X}) \to (\mathtt{T2} \to \mathtt{X}) \to \mathtt{X});$

$\mathtt{List} = \lambda \mathtt{T}.\ (\forall \mathtt{x}.\ (\mathtt{T} \to \mathtt{X} \to \mathtt{X}) \to \mathtt{X} \to \mathtt{X});$

Type-Level Computation

Principle (Type-Level Computation)

λ-abstraction is **THE** mechanism of defining computation.

```
Pair = λT1. λT2. (∀X. (T1→T2→X) → X);
Sum = λT1. λT2. (∀X. (T1→X) → (T2→X) → X);
List = λT. (∀x. (T→X→X) → X → X);
```

We introduce λX. T to abstract **types** out of **types**.

Observation

Type-level computation allows writing the **same** type in **different** ways.

Example

Consider `Id = λX. X`. The following types are equivalent:

`Nat→Bool` `Nat→Id Bool` `Id Nat→Id Bool` `Id Nat→Bool` `Id (Nat→Bool)`

Type-Level Abstraction & Application

Syntax

$$\mathsf{T} ::= \mathsf{X} \mid \lambda\mathsf{X}.\,\mathsf{T} \mid \mathsf{T}\ \mathsf{T} \mid \mathsf{T} \to \mathsf{T} \mid \mathtt{Bool} \mid \mathtt{Nat} \mid \ldots$$

$$\mathsf{TV} ::= \lambda\mathsf{X}.\,\mathsf{T} \mid \mathsf{TV} \to \mathsf{TV} \mid \mathtt{Bool} \mid \mathtt{Nat} \mid \ldots$$

Evaluation: $\mathsf{T} \longrightarrow \mathsf{T}'$

$$\frac{\mathsf{T}_1 \longrightarrow \mathsf{T}_1'}{\mathsf{T}_1\ \mathsf{T}_2 \longrightarrow \mathsf{T}_1'\ \mathsf{T}_2} \qquad \frac{\mathsf{T}_2 \longrightarrow \mathsf{T}_2'}{\mathsf{TV}_1\ \mathsf{T}_2 \longrightarrow \mathsf{TV}_1\ \mathsf{T}_2'} \qquad \frac{}{(\lambda\mathsf{X}.\,\mathsf{T}_{12})\ \mathsf{TV}_2 \longrightarrow [\mathsf{X} \mapsto \mathsf{TV}_2]\mathsf{T}_{12}}$$

$$\frac{\mathsf{T}_1 \longrightarrow \mathsf{T}_1'}{(\mathsf{T}_1 \to \mathsf{T}_2) \longrightarrow (\mathsf{T}_1' \to \mathsf{T}_2)} \qquad \frac{\mathsf{T}_2 \longrightarrow \mathsf{T}_2'}{(\mathsf{TV}_1 \to \mathsf{T}_2) \longrightarrow (\mathsf{TV}_1 \to \mathsf{T}_2')}$$

Question

It seems that we formulate a type-level **untyped** lambda calculus. **Any issues?**

Issue 1: Unequal Equivalent Types

Example

Consider `Id = λX. X`. Two type-level values `λX. Id X` and `λX. X` are **unequal** but **equivalent**.

Observation

We do not care about how types evaluate.
We care about if they are equivalent.

Equivalence: $S \equiv T$

$$\frac{}{T \equiv T} \qquad \frac{T \equiv S}{S \equiv T} \qquad \frac{S \equiv U \qquad U \equiv T}{S \equiv T} \qquad \frac{S_1 \equiv T_1 \qquad S_2 \equiv T_2}{S_1 \to S_2 \equiv T_1 \to T_2}$$

$$\frac{S_2 \equiv T_2}{\lambda X.\, S_2 \equiv \lambda X.\, T_2} \qquad \frac{S_1 \equiv T_1 \qquad S_2 \equiv T_2}{S_1\; S_2 \equiv T_1\; T_2} \qquad \frac{}{(\lambda X.\, T_{12})\; T_2 \equiv [X \mapsto T_2]T_{12}}$$

Issue 2: Errors in Type-Level Computation

Example

Consider $(\lambda\,\mathtt{X}.\ \mathtt{X}\ \mathtt{X})\ \mathtt{Nat}$. The type evaluates to $\mathtt{Nat}\ \mathtt{Nat}$, which is an **illy-formed** type.
Consider $(\lambda\,\mathtt{X}.\ \mathtt{X}\ \mathtt{X})\ (\lambda\,\mathtt{X}.\ \mathtt{X}\ \mathtt{X})$. The type's evaluation **diverges**.

Principle (Characterization of Type-Level Computation)

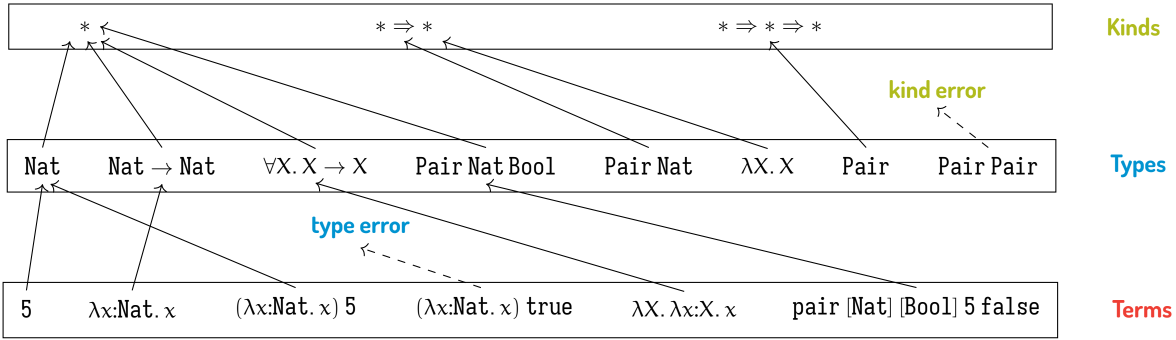
Recall that **types** characterize **terms**.
What can characterize **types**?

Kinds: "Types of Types"

Kinds characterize **types**.

$*$	proper types (e.g., $\mathtt{Bool}$ and $\mathtt{Nat} \to \mathtt{Bool}$)
$* \Rightarrow *$	type operators, i.e., functions from proper types to proper types
$* \Rightarrow * \Rightarrow *$	functions from proper types to type operators, i.e., two-argument operators
$(* \Rightarrow *) \Rightarrow *$	functions from type operators to proper types

Terms, Types, and Kinds



Question

- What is the difference between $\forall X.\, X \to X$ and $\lambda X.\, X \to X$?
- Why doesn't an arrow type $\mathtt{Nat} \to \mathtt{Nat}$ have an arrow kind like $* \Rightarrow *$?

Kinding

Syntax

$$T ::= X \mid \lambda X{::}K.\, T \mid T\ T \mid T \to T \mid \texttt{Bool} \mid \texttt{Nat} \mid \ldots$$

$$K ::= * \mid K \Rightarrow K \qquad\qquad \Gamma ::= \varnothing \mid \Gamma, x : T \mid X :: K$$

$\Gamma \vdash T :: K$: "type T has kind K in context Γ"

$$\frac{X :: K \in \Gamma}{\Gamma \vdash X :: K} \qquad \frac{\Gamma, X :: K_1 \vdash T_2 :: K_2}{\Gamma \vdash \lambda X{::}K_1.\, T_2 :: K_1 \Rightarrow K_2} \qquad \frac{\Gamma \vdash T_1 :: K_{11} \Rightarrow K_{12} \qquad \Gamma \vdash T_2 :: K_{11}}{\Gamma \vdash T_1\ T_2 :: K_{12}}$$

$$\frac{\Gamma \vdash T_1 :: * \qquad \Gamma \vdash T_2 :: *}{\Gamma \vdash T_1 \to T_2 :: *} \qquad \frac{}{\Gamma \vdash \texttt{Bool} :: *} \qquad \frac{}{\Gamma \vdash \texttt{Nat} :: *}$$

Observation

The **kinding** relation $\Gamma \vdash T :: K$ is very similar to the **typing** relation $\Gamma \vdash t : T$.

$\lambda_\omega = \lambda_\rightarrow$ + Type Operators

t	$::=$		*terms:*
		x	*variable*
		$\lambda x{:}T.\, t$	*abstraction*
		$t\ t$	*application*
v	$::=$		*values:*
		$\lambda x{:}T.\, t$	*abstraction value*
T	$::=$		*types:*
		X	*type variable*
		$\lambda X{::}K.\, T$	*operator abstraction*
		$T\ T$	*operator application*
		$T \to T$	*type of functions*
Γ	$::=$		*contexts:*
		$\varnothing$	*empty context*
		$\Gamma, x : T$	*term variable binding*
		$\Gamma, X :: K$	*type variable binding*
K	$::=$		*kinds:*
		$*$	*kind of proper types*
		$K \Rightarrow K$	*kind of operators*

Typing

Typing

$$\frac{x : T \in \Gamma}{\Gamma \vdash x : T} \qquad \frac{\Gamma \vdash T_1 :: * \qquad \Gamma, x : T_1 \vdash t_2 : T_2}{\Gamma \vdash \lambda x{:}T_1 .\, t_2 : T_1 \to T_2} \qquad \frac{\Gamma \vdash t_1 : T_{11} \to T_{12} \qquad \Gamma \vdash t_2 : T_{11}}{\Gamma \vdash t_1\ t_2 : T_{12}}$$

$$\frac{\Gamma \vdash t : S \qquad S \equiv T \qquad \Gamma \vdash T :: *}{\Gamma \vdash t : T}$$

Observation

If $\varnothing \vdash t : T$, then $\varnothing \vdash T :: *$.

Question

How to decide type equivalence $S \equiv T$ **algorithmically**?

Approach 1: Parallel Reduction

$S \Rrightarrow T$: "type S parallelly reduces to type T"

$$\frac{}{T \Rrightarrow T} \qquad \frac{S_1 \Rrightarrow T_1 \qquad S_2 \Rrightarrow T_2}{S_1 \to S_2 \Rrightarrow T_1 \to T_2} \qquad \frac{S_2 \Rrightarrow T_2}{\lambda X{::}K_1.\, S_2 \Rrightarrow \lambda X{::}K_1.\, T_2} \qquad \frac{S_1 \Rrightarrow T_1 \qquad S_2 \Rrightarrow T_2}{S_1\ S_2 \Rrightarrow T_1\ T_2}$$

$$\frac{S_{12} \Rrightarrow T_{12} \qquad S_2 \Rrightarrow T_2}{(\lambda X{::}K_{11}.\, S_{12})\ S_2 \Rrightarrow [X \mapsto T_2]T_{12}}$$

Example

Let $S \stackrel{\text{def}}{=} \mathtt{Id}\,\mathtt{Nat} \to \mathtt{Bool}$ and $T \stackrel{\text{def}}{=} \mathtt{Id}\,(\mathtt{Nat} \to \mathtt{Bool})$. Then

$$S = ((\lambda X{::}*.\, X)\ \mathtt{Nat}) \to \mathtt{Bool} \Rrightarrow \mathtt{Nat} \to \mathtt{Bool}, \qquad T = (\lambda X{::}*.\, X)\ (\mathtt{Nat} \to \mathtt{Bool}) \Rrightarrow \mathtt{Nat} \to \mathtt{Bool}.$$

Theorem

$S \equiv T$ **if and only if** there exists some U such that $S \Rrightarrow^* U$ and $T \Rrightarrow^* U$.

Approach 2: Weak-Head Reduction

$S \rightsquigarrow T$: "type S weak-head reduces to type T"

Weak-head reduction only reduces **outermost** type-level applications.

$$\frac{T_1 \rightsquigarrow T_1'}{T_1\ T_2 \rightsquigarrow T_1'\ T_2} \qquad \frac{}{(\lambda X{::}K.\ T_{12})\ T_2 \rightsquigarrow [X \mapsto T_2]T_{12}}$$

We denote by $S \Downarrow T$ to mean "type S weak-head normalizes to type T."

$$\frac{T \not\rightsquigarrow}{T \Downarrow T} \qquad \frac{S \rightsquigarrow T \qquad T \Downarrow T'}{S \Downarrow T'}$$

$\Gamma \vdash S \Leftrightarrow T :: K$ and $\Gamma \vdash S \leftrightarrow T :: K$: Algorithmic and Structural Equivalence

$$\frac{S \Downarrow S' \qquad T \Downarrow T' \qquad \Gamma \vdash S \leftrightarrow T :: *}{\Gamma \vdash S \Leftrightarrow T :: *} \qquad \frac{X \notin \Gamma \qquad \Gamma, X :: K_1 \vdash S\ X \Leftrightarrow T\ X :: K_2}{\Gamma \vdash S \Leftrightarrow T :: K_1 \Rightarrow K_2}$$

$$\frac{X :: K \in \Gamma}{\Gamma \vdash X \leftrightarrow X :: K} \qquad \frac{\Gamma \vdash S_1 \leftrightarrow T_1 :: * \qquad \Gamma \vdash S_2 \leftrightarrow T_2 :: *}{\Gamma \vdash S_1 \to S_2 \leftrightarrow T_1 \to T_2 :: *} \qquad \frac{\Gamma \vdash S_1 \leftrightarrow T_1 :: K_1 \Rightarrow K_2 \qquad \Gamma \vdash S_2 \Leftrightarrow T_2 :: K_1}{\Gamma \vdash S_1\ S_2 \leftrightarrow T_1\ T_2 :: K_2}$$

Parallel Reduction vs. Weak-Head Reduction

Example

```
Pair = λY::*. {Y,Y};
List = λY::*. (μX. <nil:Unit,cons:{Y,X}>);
```

Determine that `List(List(Pair(Nat)))` and `List(List({Nat,Nat}))` are equivalent.

Parallel Reduction

$$\texttt{List}(\texttt{List}(\texttt{Pair}(\texttt{Nat}))) \Rrightarrow^* \mu X.\, \texttt{<nil:Unit}, \texttt{cons:}\{\mu Y.\, \texttt{<nil:Unit}, \texttt{cons:}\{\{\texttt{Nat}, \texttt{Nat}\}, Y\}\texttt{>}, X\}\texttt{>}$$

$$\texttt{List}(\texttt{List}(\{\texttt{Nat}, \texttt{Nat}\})) \Rrightarrow^* \mu X.\, \texttt{<nil:Unit}, \texttt{cons:}\{\mu Y.\, \texttt{<nil:Unit}, \texttt{cons:}\{\{\texttt{Nat}, \texttt{Nat}\}, Y\}\texttt{>}, X\}\texttt{>}$$

Parallel Reduction vs. Weak-Head Reduction

Example

```
Pair = λY::*. {Y,Y};
List = λY::*. (μX. <nil:Unit,cons:{Y,X}>);
```

Determine that `List(List(Pair(Nat)))` and `List(List({Nat,Nat}))` are equivalent.

Weak-Head Reduction

We start with $\varnothing \vdash \texttt{List}(\texttt{List}(\texttt{Pair}(\texttt{Nat}))) \Leftrightarrow \texttt{List}(\texttt{List}(\{\texttt{Nat}, \texttt{Nat}\})) :: *$.

$$\texttt{List}(\texttt{List}(\texttt{Pair}(\texttt{Nat}))) \Downarrow \mu\texttt{X}.\, \texttt{<nil:Unit}, \texttt{cons:}\{\texttt{List}(\texttt{Pair}(\texttt{Nat})), \texttt{X}\}\texttt{>}$$
$$\texttt{List}(\texttt{List}(\{\texttt{Nat}, \texttt{Nat}\})) \Downarrow \mu\texttt{X}.\, \texttt{<nil:Unit}, \texttt{cons:}\{\texttt{List}(\{\texttt{Nat}, \texttt{Nat}\}), \texttt{X}\}\texttt{>}$$

By structural equivalence, we resort to check $\varnothing \vdash \texttt{Pair}(\texttt{Nat}) \Leftrightarrow \{\texttt{Nat}, \texttt{Nat}\} :: *$.

$$\texttt{Pair}(\texttt{Nat}) \Downarrow \{\texttt{Nat}, \texttt{Nat}\}$$
$$\{\texttt{Nat}, \texttt{Nat}\} \Downarrow \{\texttt{Nat}, \texttt{Nat}\}$$

System F_ω: The Combination of System F and λ_ω

Syntax

$$
\begin{aligned}
t &::= x \mid \lambda x{:}T.\, t \mid t\ t \mid \lambda X{::}K.\, t \mid t\ [T] \mid \{{}^*T, t\} \text{ as } T \mid \texttt{let}\ \{X, x\} = t\ \texttt{in}\ t \\
v &::= \lambda x{:}T.\, t \mid \lambda X{::}K.\, t \mid \{{}^*T, v\} \text{ as } T \\
T &::= X \mid \lambda X{::}K.\, T \mid T\ T \mid T \to T \mid \forall X{::}K.\, T \mid \{\exists X{::}K, T\} \\
\Gamma &::= \varnothing \mid \Gamma, x : T \mid \Gamma, X :: K \\
K &::= * \mid K \Rightarrow K
\end{aligned}
$$

Observation

- The universal type $\forall X.\, T$ becomes $\forall X{::}K.\, T$, i.e., we can abstract terms out of **type operators**.
- The existential type $\{\exists X, T\}$ becomes $\{\exists X{::}K, T\}$, i.e., we can pack a term to hide some **type operator**.

Typing, Kinding, and Type Equivalence

Typing

$$\frac{\Gamma, X :: K_1 \vdash t_2 : T_2}{\Gamma \vdash \lambda X{::}K_1 . t_2 : \forall X{::}K_1 . T_2}$$

$$\frac{\Gamma \vdash t_1 : \forall X{::}K_{11} . T_{12} \qquad \Gamma \vdash T_2 :: K_{11}}{\Gamma \vdash t_1\ [T_2] : [X \mapsto T_2]T_{12}}$$

$$\frac{\Gamma \vdash t_2 : [X \mapsto U]T_2 \qquad \Gamma \vdash \{\exists X{::}K_1, T_2\} :: *}{\Gamma \vdash \{{}^*U, t_2\} \text{ as } \{\exists X{::}K_1, T_2\} : \{\exists X{::}K_1, T_2\}}$$

$$\frac{\begin{array}{c}\Gamma \vdash t_1 : \{\exists X{::}K_{11}, T_{12}\} \\ \Gamma, X{::}K_{11}, x : T_{12} \vdash t_2 : T_2\end{array}}{\Gamma \vdash \mathtt{let}\ \{X, x\} = t_1\ \mathtt{in}\ t_2 : T_2}$$

Kinding and Type Equivalence

$$\frac{\Gamma, X :: K_1 \vdash T_2 :: *}{\Gamma \vdash \forall X{::}K_1 . T_2 :: *}$$

$$\frac{\Gamma, X :: K_1 \vdash T_2 :: *}{\Gamma \vdash \{\exists X{::}K_1, T_2\} :: *}$$

$$\frac{S_2 \equiv T_2}{\forall X{::}K_1 . S_2 \equiv \forall X{::}K_1 . T_2}$$

$$\frac{S_2 \equiv T_2}{\{\exists X{::}K_1, S_2\} \equiv \{\exists X{::}K_1, T_2\}}$$

Review: Abstract Data Types (ADTs)

Definition

An abstract data type (ADT) consists of

- a type name `A`,
- a concrete representation type `T`,
- implementations of operations for manipulating values of type `T`, and
- an **abstraction boundary** enclosing the representation and operations.

```
counterADT =
   {*Nat, {new = 1,
           get = λi:Nat. i,
           inc = λi:Nat. succ(i)}}
 as {∃Counter,
      {new: Counter, get: Counter→Nat, inc: Counter→Counter}};
▶ counterADT : {∃Counter,
                 {new:Counter,get:Counter→Nat,inc:Counter→Counter}}
```

Abstract Type Operators

Question

We want to implement an ADT of pairs.

- The ADT provides operations for building pairs and taking them apart.
- Those operations need to be **polymorphic**.

The abstract type `Pair` would not be a proper type, but an **abstract type operator**!

$$
\begin{aligned}
\texttt{PairSig} = \{\exists\,\texttt{Pair} :: * \Rightarrow * \Rightarrow *,\ & \\
\{\texttt{pair}:\ & \forall \texttt{X}.\ \forall \texttt{Y}.\ \texttt{X} \to \texttt{Y} \to (\texttt{Pair X Y}), \\
\texttt{fst}\ :\ & \forall \texttt{X}.\ \forall \texttt{Y}.\ (\texttt{Pair X Y}) \to \texttt{X}, \\
\texttt{snd}\ :\ & \forall \texttt{X}.\ \forall \texttt{Y}.\ (\texttt{Pair X Y}) \to \texttt{Y}\}\};
\end{aligned}
$$

Abstract Type Operators

Example

```
pairADT = {*(λX. λY. ∀R. (X→Y→R) → R),
              {pair = λX. λY. λx:X. λy:Y. λR. λp:(X→Y→R). p x y,
               fst  = λX. λY. λp:(∀R. (X→Y→R) → R). p [X] (λx:X. λy:Y. x),
               snd  = λX. λY. λp:(∀R. (X→Y→R) → R). p [Y] (λx:X. λy:Y. y)}}
             as PairSig;
▶ pairADT : PairSig

let {Pair,pair} = pairADT
in pair.fst [Nat] [Bool] (pair.pair [Nat] [Bool] 5 true);
▶ 5 : Nat
```

More Examples

`Option`: Combination with Variants

```
Option = λX. <none:Unit,some:X>;
none = λX. <none=unit> as (Option X);
▶ none : ∀X. (Option X)
some = λX. λx:X. <some=x> as (Option X);
▶ some : ∀X. X → (Option X)
```

`List`: Combination with Variants, Tuples, and Recursive Types

```
List = μL::(*⇒*). λX. <nil:Unit,cons:{X,(L X)}>;
nil = λX. <nil=unit> as (List X);
▶ nil : ∀X. (List X)
cons = λX. λh:X. λt:(List X). <cons={h,t}> as (List X);
▶ cons : ∀X. X → (List X) → (List X)
```

More Examples

Queue: Implementing a Queue using Two Lists

```
QueueSig = {∃Q :: *⇒*,
            {empty : ∀X. (Q X),
             insert: ∀X. X → (Q X) → (Q X),
             remove: ∀X. (Q X) → Option {X,(Q X)}}};
queueADT = {*(λX. {List X,List X}),
            {empty  = λX. {nil [X],nil [X]},
             insert = λX. λa:X. λq:{List X,List X}. {(cons [X] a q.1),q.2},
             remove =
              λX. λq:{List X,List X}.
               let q' = case q.2 of <nil=u> ⇒ {nil [X], reverse [X] q.1}
                                  | <cons={h,t}> ⇒ q
               in case q'.2 of
                 <nil=u> ⇒ none [{X,{List X,List X}}]
               | <cons={h,t}> ⇒ some [{X,{List X,List X}}] {h,{q'.1,t}}}} as QueueSig;
▶ queueADT : QueueSig
```

Preservation

Observation

The structural rule (T-Eq) makes induction proof difficult:

$$\frac{\Gamma \vdash t : S \qquad S \equiv T \qquad \Gamma \vdash T :: *}{\Gamma \vdash t : T}$$

Preservation of Shapes (for Arrows)

If $S_1 \to S_2 \Rrightarrow^* T$, then $T = T_1 \to T_2$ with $S_1 \Rrightarrow^* T_1$ and $S_2 \Rrightarrow^* T_2$.

Inversion (for Arrows)

If $\Gamma \vdash \lambda x{:}S_1 .\, s_2 : T_1 \to T_2$, then $T_1 \equiv S_1$ and $\Gamma, x : S_1 \vdash s_2 : T_2$. Also $\Gamma \vdash S_1 :: *$.

Theorem (30.3.14)

If $\Gamma \vdash t : T$ and $t \longrightarrow t'$, then $\Gamma \vdash t' : T$.

Progress

Canonical Forms (for Arrows)

If t is a closed value with $\varnothing \vdash t : T_1 \to T_2$, then t is an abstraction.

Theorem (30.3.16)

Suppose t is a closed, well-typed term (that is, $\varnothing \vdash t : T$ for some T).
Then either t is a value or else there is some t' with $t \longrightarrow t'$.

Kinding

Remark

Recall that we observed that if $\varnothing \vdash t : T$, then $\varnothing \vdash T :: *$.

Context Formation

$$\frac{}{\varnothing \text{ ctx}} \qquad \frac{\Gamma \text{ ctx} \qquad \Gamma \vdash T :: *}{\Gamma, x : T \text{ ctx}} \qquad \frac{\Gamma \text{ ctx}}{\Gamma, X :: K \text{ ctx}}$$

Theorem

If Γ ctx and $\Gamma \vdash t : T$, then $\Gamma \vdash T :: *$.

Fragments of System F_ω

Definition

In System F_1, the only kind is $*$ and no quantification ($\forall$) or abstraction (λ) over types is permitted.
The remaining systems are defined with reference to a hierarchy of kinds at **level** i:

$$\begin{aligned}
\mathcal{K}_1 &= \varnothing \\
\mathcal{K}_{i+1} &= \{*\} \cup \{J \Rightarrow K \mid J \in \mathcal{K}_i \wedge K \in \mathcal{K}_{i+1}\} \\
\mathcal{K}_\omega &= \bigcup_{1 \leqslant i} \mathcal{K}_i
\end{aligned}$$

Example

- System F_1 is the simply-typed lambda-calculus $\lambda_\to$.
- In System F_2, we have $\mathcal{K}_2 = \{*\}$, so there is no lambda-abstraction at the type level but we allow quantification over proper types.
  - F_2 is just the System F; this is why System F is also called the **second-order lambda-calculus**.
- For System F_3, we have $\mathcal{K}_3 = \{*, * \Rightarrow *, * \Rightarrow * \Rightarrow *, \ldots\}$, i.e., type-level abstractions are over proper types.

Type-Level Natural Numbers

Remark

The kinding system of λ_ω and F_ω consists of only $*$ and $K_1 \Rightarrow K_2$.
Can we extend kinding to support more versatile type-level computation?

Observation

We can extend type-level computation as long as **type equivalence remains decidable**.

Natural-Number Kind

$$K ::= * \mid K \Rightarrow K \mid \mathbb{N}$$

$$T ::= X \mid \lambda X{::}K.\ T \mid T\ T \mid T \to T \mid \forall X{::}K.\ T \mid \{\exists X{::}K, T\} \mid \mathtt{ZERO} \mid \mathtt{SUCC}\ T \mid \ldots$$

With recursive types, we can define length-indexed lists:

```
List = λX. μL :: (ℕ ⇒ *). λM :: ℕ. IF ISZERO(M) THEN Unit ELSE {X,(L (PRED M))};
▶ List :: * ⇒ ℕ ⇒ *
```

Type-Level Natural Numbers

Example

```
List = λX. μL::(ℕ⇒*). λM::ℕ. IF ISZERO(M) THEN Unit ELSE {X,(L (PRED M))};
▶ List :: * ⇒ ℕ ⇒ *

nil = λX. unit as (List X ZERO);
▶ nil : ∀X. (List X Zero)
cons = λX. λM::ℕ. λh:X. λt:(List X M). {h,t} as (List X (SUCC M));
▶ cons : ∀X. ∀M::ℕ. X → (List X M) → (List X (SUCC M))
```

Example

```
PLUS = μP::(ℕ⇒ℕ⇒ℕ). λM::ℕ. λN::ℕ. IF ISZERO(M) THEN N ELSE P (PRED M) N;
▶ PLUS :: ℕ ⇒ ℕ ⇒ ℕ
```

Type-Level Natural Numbers

Natural-Number Kind

Type-level recursion would render type equivalence **undecidable**.
Let us consider $\mathbb{N}$ as an **inductively-defined** kind.

$$\mathsf{T} ::= \mathsf{X} \mid \lambda \mathsf{X}::\mathsf{K}.\,\mathsf{T} \mid \mathsf{T}\ \mathsf{T} \mid \mathsf{T} \to \mathsf{T} \mid \forall \mathsf{X}::\mathsf{K}.\,\mathsf{T} \mid \{\exists \mathsf{X}::\mathsf{K}, \mathsf{T}\} \mid \mathtt{ZERO} \mid \mathtt{SUCC}\ \mathsf{T} \mid \mathtt{ITER}\ \mathsf{T}\ \mathtt{WITH}\ \mathtt{ZERO} \Rightarrow \mathsf{T} \mid \mathtt{SUCC} \Rightarrow \mathsf{Y}.\,\mathsf{T}$$

Below are the kinding rules for $\mathbb{N}$:

$$\frac{}{\Gamma \vdash \mathtt{ZERO} :: \mathbb{N}} \qquad \frac{\Gamma \vdash \mathsf{T}_1 :: \mathbb{N}}{\Gamma \vdash \mathtt{SUCC}\ \mathsf{T}_1 :: \mathbb{N}} \qquad \frac{\Gamma \vdash \mathsf{T}_0 :: \mathbb{N} \qquad \Gamma \vdash \mathsf{T}_1 :: \mathsf{K} \qquad \Gamma, \mathsf{Y} :: \mathsf{K} \vdash \mathsf{T}_2 :: \mathsf{K}}{\Gamma \vdash \mathtt{ITER}\ \mathsf{T}_0\ \mathtt{WITH}\ \mathtt{ZERO} \Rightarrow \mathsf{T}_1 \mid \mathtt{SUCC} \Rightarrow \mathsf{Y}.\,\mathsf{T}_2 :: \mathsf{K}}$$

Example

```
List = λX. λM::ℕ. ITER M OF ZERO ⇒ Unit | SUCC ⇒ Y. {X,Y};
▶ List :: * ⇒ ℕ ⇒ *
PLUS = λM::ℕ. λN::ℕ. ITER M OF ZERO ⇒ N | SUCC ⇒ Y. SUCC Y;
▶ PLUS :: ℕ ⇒ ℕ ⇒ ℕ
```

Type-Level Natural Numbers

Term-Level Case on Type-Level Natural Numbers

$$\frac{\Gamma \vdash T_0 :: \mathbb{N} \qquad \Gamma, T_0 \equiv \mathsf{ZERO} :: \mathbb{N} \vdash t_1 : T \qquad \Gamma, Y :: \mathbb{N}, T_0 \equiv \mathsf{SUCC}\ Y :: \mathbb{N} \vdash t_2 : T \qquad \Gamma \vdash T :: *}{\Gamma \vdash \mathsf{tcase}\ T_0\ \mathsf{of}\ \mathsf{ZERO} \Rightarrow t_1 \mid \mathsf{SUCC}\ Y \Rightarrow t_2 : T}$$

Example

```
List = λX. λM::ℕ. ITER M OF ZERO ⇒ Unit | SUCC ⇒ Y. {X,Y};
▶ List :: * ⇒ ℕ ⇒ *
PLUS = λM::ℕ. λN::ℕ. ITER M OF ZERO ⇒ N | SUCC ⇒ Y. SUCC Y;
▶ PLUS :: ℕ ⇒ ℕ ⇒ ℕ

▶ append : ∀X. ∀M::ℕ. ∀N::ℕ. (List X M) → (List X N) → (List X (PLUS M N))
append = λX. fix λf. λM::ℕ. λN::ℕ. λl1:(List X M). λl2:(List X N).
           tcase M of ZERO ⇒ let unit  = l1 in l2 as (List X (PLUS M N))
                   SUCC M' ⇒ let {h,t} = l1 in {h,(f M' N t l2)} as (List X (PLUS M N));
```

Type-Level Natural Numbers

Remark

Because type-equivalence constraints can appear in the context, we need **hypothetical** type equivalence.
Ref: J. Cheney and R. Hinze. 2003. First-Class Phantom Types. Technical report. Cornell University.

Hypothetical Type Equivalence: $\Gamma \vdash S \equiv T :: K$

$$\frac{\Gamma \vdash T :: K}{\Gamma \vdash T \equiv T :: K} \qquad \frac{\Gamma \vdash T \equiv S :: K}{\Gamma \vdash S \equiv T :: K} \qquad \frac{\Gamma \vdash S \equiv U :: K \qquad \Gamma \vdash U \equiv T :: K}{\Gamma \vdash S \equiv T :: K}$$

$$\frac{\Gamma \vdash S_1 \equiv T_1 :: * \qquad \Gamma \vdash S_2 \equiv T_2 :: *}{\Gamma \vdash S_1 \to S_2 \equiv T_1 \to T_2 :: *} \qquad \frac{\Gamma, X :: K_1 \vdash S_2 \equiv T_2 :: K_2}{\Gamma \vdash \lambda X{::}K_1 . S_2 \equiv \lambda X{::}K_1 . T_2 :: K_1 \Rightarrow K_2}$$

$$\frac{\Gamma \vdash S_1 \equiv T_1 :: K_{11} \Rightarrow K_{12} \qquad \Gamma \vdash S_2 \equiv T_2 :: K_{11}}{\Gamma \vdash S_1\ S_2 \equiv T_1\ T_2 :: K_{12}} \qquad \frac{\Gamma, X :: K_{11} \vdash T_{12} :: K_{12} \qquad \Gamma \vdash T_2 :: K_{11}}{\Gamma \vdash (\lambda X{::}K_{11} . T_{12})\ T_2 \equiv [X \mapsto T_2]T_{12} :: K_{12}}$$

Type-Level Natural Numbers

Hypothetical Type Equivalence: $\Gamma \vdash S \equiv T :: K$

$$\frac{}{\Gamma \vdash \mathtt{ZERO} \equiv \mathtt{ZERO} :: \mathbb{N}} \qquad \frac{\Gamma \vdash S_1 \equiv T_1 :: \mathbb{N}}{\Gamma \vdash \mathtt{SUCC}\ S_1 \equiv \mathtt{SUCC}\ T_1 :: \mathbb{N}}$$

$$\frac{\Gamma \vdash S_0 \equiv T_0 :: \mathbb{N} \qquad \Gamma \vdash S_1 \equiv T_1 :: K \qquad \Gamma, Y :: K \vdash S_2 \equiv T_2 :: K}{\Gamma \vdash \mathtt{ITER}\ S_0\ \mathtt{WITH}\ \mathtt{ZERO} \Rightarrow S_1 \mid \mathtt{SUCC} \Rightarrow Y.\, S_2 \equiv \mathtt{ITER}\ T_0\ \mathtt{WITH}\ \mathtt{ZERO} \Rightarrow T_1 \mid \mathtt{SUCC} \Rightarrow Y.\, T_2 :: K}$$

$$\frac{\Gamma \vdash T_1 :: K \qquad \Gamma, Y :: K \vdash T_2 :: K}{\Gamma \vdash \mathtt{ITER}\ \mathtt{ZERO}\ \mathtt{WITH}\ \mathtt{ZERO} \Rightarrow T_1 \mid \mathtt{SUCC} \Rightarrow Y.\, T_2 \equiv T_1 :: K}$$

$$\frac{\Gamma \vdash T_0 :: \mathbb{N} \qquad \Gamma \vdash T_1 :: K \qquad \Gamma, Y :: K \vdash T_2 :: K}{\begin{array}{c}\Gamma \vdash \mathtt{ITER}\ (\mathtt{SUCC}\ T_0)\ \mathtt{WITH}\ \mathtt{ZERO} \Rightarrow T_1 \mid \mathtt{SUCC} \Rightarrow Y.\, T_2 \\ \equiv \\ [Y \mapsto \mathtt{ITER}\ T_0\ \mathtt{WITH}\ \mathtt{ZERO} \Rightarrow T_1 \mid \mathtt{SUCC} \Rightarrow Y.\, T_2]T_2 :: K\end{array}}$$

Type-Level Natural Numbers

Hypothetical Type Equivalence: $\Gamma \vdash S \equiv T :: K$

$$\frac{S \equiv T :: \mathbb{N} \in \Gamma}{\Gamma \vdash S \equiv T :: \mathbb{N}} \qquad \frac{\Gamma \vdash \mathtt{SUCC}\ S_1 \equiv \mathtt{SUCC}\ T_1 :: \mathbb{N}}{\Gamma \vdash S_1 \equiv T_1 :: \mathbb{N}}$$

Example

$$\mathtt{append} \equiv \lambda X.\ \mathbf{fix}\ \lambda f{:}\_.\ \lambda M{::}\mathbb{N}.\ \lambda N{::}\mathbb{N}.\ \lambda l_1{:}(\mathtt{List}\ X\ M).\ \lambda l_2{:}(\mathtt{List}\ X\ N).$$
$$\mathtt{tcase}\ M\ \mathtt{of}\ \mathtt{ZERO} \Rightarrow \mathtt{t1} \mid \mathtt{SUCC}\ M' \Rightarrow \mathtt{t2}$$
$$\mathtt{t1} \equiv \mathtt{let}\ \mathtt{unit} = l_1\ \mathtt{in}\ l_2\ \mathtt{as}\ (\mathtt{List}\ X\ (\mathtt{PLUS}\ M\ N))$$
$$\mathtt{t2} \equiv \mathtt{let}\ \{h, t\} = l_1\ \mathtt{in}\ \{h, (f\ M'\ N\ t\ l_2)\}\ \mathtt{as}\ (\mathtt{List}\ X\ (\mathtt{PLUS}\ M\ N))$$

Let $T_{app} \equiv \forall X{::}{*}.\ \forall M{::}\mathtt{Nat}.\ \forall N{::}\mathtt{Nat}.\ (\mathtt{List}\ X\ M) \to (\mathtt{List}\ X\ N) \to (\mathtt{List}\ X\ (\mathtt{PLUS}\ M\ N))$. We need to check

$$X :: *, f : T_{app}, M :: \mathbb{N}, N :: \mathbb{N}, l_1 : \mathtt{List}\ X\ M, l_2 : \mathtt{List}\ X\ N, M \equiv \mathtt{ZERO} :: \mathbb{N} \vdash \mathtt{t1} : \mathtt{List}\ X\ (\mathtt{PLUS}\ M\ N)$$
$$X{::}{*}, f{:}T_{app}, M{::}\mathbb{N}, N{::}\mathbb{N}, l_1{:}\mathtt{List}\ X\ M, l_2{:}\mathtt{List}\ X\ N, M'{::}\mathbb{N}, M \equiv \mathtt{SUCC}\ M' :: \mathbb{N} \vdash \mathtt{t2} : \mathtt{List}\ X\ (\mathtt{PLUS}\ M\ N)$$

Extensible Records

Remark

In Chap. 11, we studied records, i.e., named tuples, which are not **extensible**.

Extensible Records

- **Extension**: We can extend a record r with label ℓ and term t by $\{\ell = t \mid r\}$.

```
origin = {x = 0 | {y = 0 | {}}};
origin3 = {z = 0 | origin};
named = λs. λr. {name = s | r};
```

- **Selection**: The selection operation $r.\ell$ selects the value of a label ℓ from a record r.

```
distance = λp. sqrt ((p.x * p.x) + (p.y * p.y));
distance (named "2d" origin) + distance origin3;
```

- **Restriction**: The restriction operation $r - \ell$ removes a label ℓ from a record r.

```
update_name = λr. λs. {name = s | r - name };
rename_name_nn = λr. {nn = r.name | r - name };
```

Scoped Labels

Observation

Typing extensible records needs to ensure the **safety** of the operations.

- Selection $\mathtt{r}.\ell$ and restriction $\mathtt{r} - \ell$ requires the label ℓ to be **present** in $\mathtt{r}$.
- Usually, extension $\{\ell = \mathtt{t} \mid \mathtt{r}\}$ requires the label ℓ to be **absent** in $\mathtt{r}$.

Scoped Labels

Let us consider **ordered** and **scoped** labels in records, which allow **duplicated** labels.

Ref: D. Leijen. 2005. Extensible records with scoped labels. In *Symp. on Trends in Functional Programming* (TFP'05), 297–312.

```
p = {x=2, x=true};
▶ p : {x:Nat, x:Bool}
p.x;
▶ 2 : Nat
(p - x).x;
▶ true : Bool
```

Type-Level Rows

Principle

A **row** is a list of labeled types, which can be manipulated at the type level.

$$\mathsf{K} ::= * \mid \mathsf{K} \Rightarrow \mathsf{K} \mid \mathsf{row}$$

$$\mathsf{T} ::= \mathsf{X} \mid \lambda\mathsf{X}{::}\mathsf{K}.\,\mathsf{T} \mid \mathsf{T}\ \mathsf{T} \mid \mathsf{T} \to \mathsf{T} \mid \forall\mathsf{X}{::}\mathsf{K}.\,\mathsf{T} \mid \{\exists\mathsf{X}{::}\mathsf{K}, \mathsf{T}\} \mid (\!|\,|\!) \mid (\!|\ell : \mathsf{T} \mid \mathsf{T}|\!) \mid \{\mathsf{T}\}$$

For example, the record type $\{\mathtt{x} : \mathtt{Nat}, \mathtt{y} : \mathtt{Nat}\}$ is encoded as $\{(\!|\mathtt{x} : \mathtt{Nat} \mid (\!|\mathtt{y} : \mathtt{Nat} \mid (\!|\,|\!)|\!)|\!)\}$.
Below are the kinding rules for row:

$$\frac{}{\Gamma \vdash (\!|\,|\!) :: \mathsf{row}} \qquad \frac{\Gamma \vdash \mathsf{T}_1 :: * \qquad \Gamma \vdash \mathsf{T}_2 :: \mathsf{row}}{\Gamma \vdash (\!|\ell : \mathsf{T}_1 \mid \mathsf{T}_2|\!) :: \mathsf{row}} \qquad \frac{\Gamma \vdash \mathsf{T} :: \mathsf{row}}{\Gamma \vdash \{\mathsf{T}\} :: *}$$

Well-Typed Record Operations

$$\{\ell = \_ \mid \_\} : \forall\mathsf{R}{::}\mathsf{row}.\, \forall\mathsf{X}{::}*.\, \mathsf{X} \to \{\mathsf{R}\} \to \{(\!|\ell : \mathsf{X} \mid \mathsf{R}|\!)\}$$

$$(\_.\ell) : \forall\mathsf{R}{::}\mathsf{row}.\, \forall\mathsf{X}{::}*.\, \{(\!|\ell : \mathsf{X} \mid \mathsf{R}|\!)\} \to \mathsf{X}$$

$$(\_ - \ell) : \forall\mathsf{R}{::}\mathsf{row}.\, \forall\mathsf{X}{::}*.\, \{(\!|\ell : \mathsf{X} \mid \mathsf{R}|\!)\} \to \{\mathsf{R}\}$$

Row Equivalence

Question

The type $\forall R{::}\mathrm{row}.\ \forall X{::}*.\ \{(\!|\ell : X \mid R|\!)\} \to X$ of the selection operation requires ℓ to be the **first** label.
How to relax this requirement?

Type-Level Row Equivalence

$$\frac{}{(\!|\,|\!) \equiv (\!|\,|\!)} \qquad \frac{S_1 \equiv T_1 \qquad S_2 \equiv T_2}{(\!|\ell : S_1 \mid S_2|\!) \equiv (\!|\ell : T_1 \mid T_2|\!)} \qquad \frac{\ell \neq \ell'}{(\!|\ell : T_1 \mid (\!|\ell' : T_2 \mid T_3|\!)|\!) \equiv (\!|\ell' : T_2 \mid (\!|\ell : T_1 \mid T_3|\!)|\!)}$$

Example

$$\dfrac{\dfrac{\dfrac{\vdots}{\varnothing \vdash \{\mathtt{x} = \mathtt{0} \mid \{\mathtt{y} = \mathtt{true} \mid \{\}\}\} : \{(\!|\mathtt{x} : \mathtt{Nat} \mid (\!|\mathtt{y} : \mathtt{Bool} \mid (\!|\,|\!)|\!)|\!)\}} \qquad \dfrac{\mathtt{x} \neq \mathtt{y}}{\{(\!|\mathtt{x} : \mathtt{Nat} \mid (\!|\mathtt{y} : \mathtt{Bool} \mid (\!|\,|\!)|\!)|\!)\} \equiv \{(\!|\mathtt{y} : \mathtt{Bool} \mid (\!|\mathtt{x} : \mathtt{Nat} \mid (\!|\,|\!)|\!)|\!)\}}}{\varnothing \vdash \{\mathtt{x} = \mathtt{0} \mid \{\mathtt{y} = \mathtt{true} \mid \{\}\}\} : \{(\!|\mathtt{y} : \mathtt{Bool} \mid (\!|\mathtt{x} : \mathtt{Nat} \mid (\!|\,|\!)|\!)|\!)\}}}{\varnothing \vdash \{\mathtt{x} = \mathtt{0} \mid \{\mathtt{y} = \mathtt{true} \mid \{\}\}\}.\mathtt{y} : \mathtt{Bool}}$$

Use Rows for Extensible Variants

Principle

Records model labeled tuples. Variants model a labeled choice among values.

$$\mathsf{T} ::= \mathsf{X} \mid \lambda \mathsf{X}{::}\mathsf{K}.\,\mathsf{T} \mid \mathsf{T}\ \mathsf{T} \mid \mathsf{T} \to \mathsf{T} \mid \forall \mathsf{X}{::}\mathsf{K}.\,\mathsf{T} \mid \{\exists \mathsf{X}{::}\mathsf{K}, \mathsf{T}\} \mid (\!|\,|\!) \mid (\!|\ell : \mathsf{T} \mid \mathsf{T}|\!) \mid \{\mathsf{T}\} \mid \langle \mathsf{T} \rangle$$

For example, the variant type $\langle \mathtt{none} : \mathtt{Unit}, \mathtt{some} : \mathtt{Nat} \rangle$ is encoded as $\langle (\!|\mathtt{none} : \mathtt{Unit} \mid (\!|\mathtt{some} : \mathtt{Nat} \mid (\!|\,|\!)|\!)|\!) \rangle$.

Well-Typed Variant Operations

- **Injection**: We write $\langle \ell = \mathsf{t} \rangle$ to build a variant with label ℓ and term t.
  $$\langle \ell = \_ \rangle : \forall \mathsf{R}{::}\mathsf{row}.\,\forall \mathsf{X}{::}*.\,\mathsf{X} \to \langle (\!|\ell : \mathsf{X} \mid \mathsf{R}|\!) \rangle$$
- **Embedding**: We write $\langle \ell \mid v \rangle$ to embed a variant v in a type that also allows label ℓ.
  $$\langle \ell \mid \_ \rangle : \forall \mathsf{R}{::}\mathsf{row}.\,\forall \mathsf{X}{::}*.\,\langle \mathsf{R} \rangle \to \langle (\!|\ell : \mathsf{X} \mid \mathsf{R}|\!) \rangle$$
- **Decomposition**: We write $\ell \in v\ ?\ \mathsf{t}_1 : \mathsf{t}_2$ to decompose a variant v and check if it is labeled with ℓ.
  $$(\ell \in \_\ ?\ \_ : \_) : \forall \mathsf{R}{::}\mathsf{row}.\,\forall \mathsf{X}{::}*.\,\forall \mathsf{Y}{::}*.\,\langle (\!|\ell : \mathsf{X} \mid \mathsf{R}|\!) \rangle \to (\mathsf{X} \to \mathsf{Y}) \to (\langle \mathsf{R} \rangle \to \mathsf{Y}) \to \mathsf{Y}$$

Type-Level Labels

Question

Can we also introduce a kind for **labels**?

Principle

$$K ::= * \mid K \Rightarrow K \mid \text{row} \mid \text{label}$$

$$T ::= X \mid \lambda X{::}K.\,T \mid T\;T \mid T \to T \mid \forall X{::}K.\,T \mid \{\exists X{::}K, T\} \mid (\!|\,|\!) \mid (\!| T : T \mid T |\!) \mid \{T\} \mid \texttt{<}T\texttt{>} \mid \#\ell$$

$$\frac{}{\Gamma \vdash \#\ell :: \text{label}} \qquad \frac{\Gamma \vdash T_1 :: \text{label} \qquad \Gamma \vdash T_2 :: * \qquad \Gamma \vdash T_3 :: \text{row}}{\Gamma \vdash (\!| T_1 : T_2 \mid T_3 |\!) :: \text{row}}$$

Type-Level Record Computation

Question

Can we support non-trivial type-level record computation?

Principle

Ref: A. Chlipala. 2010. Ur: Statically-Typed Metaprogramming with Type-Level Record Computation. In *Prog. Lang. Design and Impl.* (PLDI'10), 122–133. doi: 10.1145/1806596.1806612.

$$T ::= X \mid \lambda X{::}K.\,T \mid T\ T \mid T \to T \mid \forall X{::}K.\,T \mid \{\exists X{::}K, T\} \mid (\!|\,|\!) \mid (\!| T : T \mid T |\!) \mid \{T\} \mid \texttt{<}T\texttt{>} \mid \#\ell \mid \texttt{map}$$

$$\frac{}{\Gamma \vdash \texttt{map} :: (* \Rightarrow *) \Rightarrow \mathsf{row} \Rightarrow \mathsf{row}}$$

Example

Consider `Meta = λT. {⦇ #name:String, #show:(T→String) ⦈}`.
Then `map Meta ⦇ #x:Nat, #y:Bool ⦈` is equivalent to `⦇ #x:(Meta Nat), #y:(Meta Bool) ⦈`.

Example: A Generic Table Formatter

```
Meta = λT. {⦇ #name:String, #show:(T→String) ⦈};
▶ Meta :: * ⇒ *

Folder = λR::row. ∀TF::(row⇒*).
              (∀L::label. ∀T. ∀R::row. TF R → TF ⦇ L : T | R ⦈) → TF ⦇⦈ → TF R;
▶ Folder :: row ⇒ *

▶ mk_table : ∀R::row. Folder R → { map Meta R } → { R } → String
mk_table = λR::row. λfl:(Folder R). λmr:{map Meta R}. λx:{R}.
      fl (λR::row. {map Meta R} → {R} → String)
         (λL::label. λT. λR::row.
            λacc:({map Meta R}→{R}→String).
            λmr:{map Meta ⦇ L : T | R ⦈}.
            λx:{⦇ L : T | R ⦈}.
"<tr><th>" ^ mr.L.name ^ "</th><td>" ^ mr.L.show x.L ^ "</td></tr>" ^ acc (mr-L) (x-L))
         (λ_:{map Meta ⦇⦈}. λ_:{⦇⦈}. "") mr x
```

Indexed Types

Observation

Previously, to support type-level natural numbers, we enrich the type level with natural-number operations.

- This approach complicates type-equivalence checking.
- This approach cannot make use of automatic solvers for natural-number reasoning.

Principle

We can separate natural numbers from the type level to reside in **its own index level**.

$$S ::= \{a :: \mathbb{N} \mid \theta\} \mid \{\theta\}$$

$$I ::= a \mid n \mid I + I \mid I \times I \mid \ldots$$

$$\theta ::= \top \mid \bot \mid \neg\theta \mid \theta \wedge \theta \mid \theta \vee \theta \mid I = I \mid I \leqslant I \mid \ldots$$

$$K ::= * \mid K \Rightarrow K \mid \mathbb{N} \Rightarrow K$$

$$T ::= X \mid \lambda X{::}L.\, T \mid T\; T \mid T \to T \mid \forall X{::}K.\, T \mid \{\exists X{::}K, T\} \mid \lambda a{::}\mathbb{N}.\, T \mid T\; I \mid \forall S.\, T \mid \{\exists S, T\}$$

Length-indexed lists: $\lambda X.\ \mu L :: (\mathbb{N}\Rightarrow *).\ \lambda M{::}\mathbb{N}.\ \{\exists \{M=0\}, \mathtt{Unit}\} + \{\exists \{M'{::}\mathbb{N} \mid M=M'+1\}, \{X, (L\ M')\}\}$.

Indexed Types

Remark

The kind $\{a : \mathbb{N} \mid \theta\}$ is usually called a **refinement** kind.
Ref: H. Xi and F. Pfenning. 1999. Dependent Types in Practical Programming. In *Princ. of Prog. Lang.* (POPL'99). doi: 10.1145/292540.292560.

Index Checking

$$\frac{\Gamma \vdash t : \forall\{a :: \mathbb{N} \mid \theta\}.\,T \qquad \Gamma \vdash i :: \{a :: \mathbb{N} \mid \theta\}}{\Gamma \vdash t\,[i] : [a \mapsto i]T} \qquad \frac{\Gamma \vdash t : \forall\{\theta\}.\,T \qquad \Gamma \vdash @ :: \{\theta\}}{\Gamma \vdash t\,[@] : T}$$

$$\frac{\Gamma \vdash [a \mapsto i]\theta}{\Gamma \vdash i :: \{a :: \mathbb{N} \mid \theta\}} \qquad \frac{\Gamma \vdash \theta}{\Gamma \vdash @ :: \{\theta\}}$$

Constraint Checking

For example, consider $\{a :: \mathbb{N} \mid a \leqslant 5\}, x : (\texttt{List Nat}\ a) \vdash \neg(a = 0)$.
We can resort to check validity of the formula in first-order logic: $\forall a : \mathbb{N}.(a \leqslant 5) \implies \neg(a = 0)$.

Homework

Question

Extend System F_ω with local type definition as follows.

$$\mathsf{t} ::= \ldots \mid \texttt{let}\ \mathsf{X} = \mathsf{T}\ \texttt{in}\ \mathsf{t}$$
$$\Gamma ::= \ldots \mid \Gamma, \mathsf{X} :: \mathsf{K} = \mathsf{T}$$

For example, the term **`let`** `X=Nat` **`in`** `(λx:X. x + 1) 4` evalutes to 5.
Extend the rules for context formation Γ ctx, type equivalence $\Gamma \vdash S \equiv \mathsf{T} :: \mathsf{K}$, kinding $\Gamma \vdash \mathsf{T} :: \mathsf{K}$, typing $\Gamma \vdash \mathsf{t} : \mathsf{T}$, and evaluation $\mathsf{t} \longrightarrow \mathsf{t}'$.