System F with Recursive and Existential Types

\[ e \equiv c \mid x \mid \lambda x : \tau. e \mid e \mid e \mid \Lambda \alpha. e \mid \Phi \alpha. \tau(e) \mid \Psi \alpha. \tau(v) \mid \Psi \alpha. \tau(v) \mid \Phi \alpha. \tau(v) \]

\[ \Delta, \Gamma \vdash e : \tau \]

System F with Recursive and Existential Types

- Metatheory (what properties does it have)
- What (else) is it good for
- How/why ML is more restrictive and implicit
- Recursive types (also use type variables, but differently)
- Existential types (dual to universal types)

Next:
- Type operators and type-level “computations”

Looking back, looking forward

Have defined System F.
Goal
Understand what this interface means and why it matters:

```plaintext
type 'a list
val empty : 'a list
val cons : 'a -> 'a list -> 'a list
val unlist : 'a list -> ('a * 'a list) option
val size : 'a list -> int
val map : ('a -> 'b) -> 'a list -> 'b list
```

Story so far:
- Recursive types to define list data structure
- Universal types to keep element type abstract in library
- Existential types to keep list type abstract in client

But, “cheated” when abstracting the list type in client: considered just intlist.

(Integer) List Library with ∃
List library is an existential package:

```plaintext
pack(μξ. unit + (int * ξ), list_library) as ∃L. {empty : L;
  cons : int → L → L;
  unlist : L → unit + (int * L);
  map : (int → int) → L → L;
  ...
}
```

The witness type is integer lists: $μξ. \text{unit} + (\text{int} * ξ)$.

The existential type variable $L$ represents integer lists.

List operations are monomorphic in element type (int).

The map function only allows mapping integer lists to integer lists.

(Polymorphic?) List Library with ∀/∃
List library is a type abstraction that yields an existential package:

```plaintext
Λα. pack(μξ. unit + (α * ξ), list_library) as ∃L. {empty : L;
  cons : α → L → L;
  unlist : L → unit + (α * L);
  map : (α → α) → L → L;
  ...
}
```

The witness type is $α$ lists: $μξ. \text{unit} + (α * ξ)$.

The existential type variable $L$ represents $α$ lists.

List operations are monomorphic in element type ($α$).

The map function only allows mapping $α$ lists to $α$ lists.

Type Abbreviations and Type Operators
Reasonable enough to provide list type as a (parametric) type abbreviation:

```plaintext
L α = μξ. unit + (α * ξ)
```

- replace occurrences of $L \tau$ in programs with $(μξ. \text{unit} + (α * ξ))[\tau/α]$

Gives an informal notion of functions at the type-level.

But, doesn’t help with with list library, because this exposes the definition of list type.

- How “modular” and “safe” are libraries built from cpp macros?
Type Abbreviations and Type Operators

Instead, provide list type as a type operator:

- a function from types to types

\[ \mathcal{L} = \lambda \alpha. \mu \xi. \text{unit} + (\alpha \times \xi) \]

Gives a formal notion of functions at the type-level.

- abstraction and application at the type-level
- equivalence of type-level expressions
- well-formedness of type-level expressions

List library will be an existential package that hides a type operator, (rather than a type).

Type-level Expressions

Abstraction and application at the type level makes it possible to write the same type with different syntax.

\[ \text{Id} = \lambda \alpha. \alpha \]

\[ \text{Id} \to \text{bool} \quad \text{int} \to \text{Id} \to \text{bool} \quad \text{Id int} \to \text{bool} \quad \text{Id} \to \text{Id} \to \text{bool} \]

\[ \text{Id (int} \to \text{bool}) \quad \text{Id (Id (int} \to \text{bool})) \]

... 

Require a precise definition of when two types are the same:

\[ \tau \equiv \tau' \]

\[ (\lambda \alpha. \tau_a) \tau_a \equiv \tau_b[\alpha/\tau_a] \]

...
Type-level Expressions

Abstraction and application at the type level makes it possible to write the same type with different syntax.

\[ \text{Id} = \lambda \alpha. \alpha \]

Admits “wrong/bad/meaningless” types:

\[ \ldots \text{bool int (Id bool) int bool (Id int)} \ldots \]

Require a “type system” for types:

\[ \Delta \vdash \tau :: \kappa \]

\[ \Delta \vdash \tau_f :: \kappa_a \Rightarrow \kappa_r \quad \Delta \vdash \tau_a :: \kappa_r \]

Terms, Types, and Kinds, Oh My

Terms: 

- atomic values (e.g., c) and operations (e.g., e + e)
- compound values (e.g., (v, v)) and operations (e.g., e . 1)
- value abstraction and application
- type abstraction and application
- classified by types (but not all terms have a type)

\[ e ::= \text{c} \mid x \mid \lambda \alpha : \tau. e \mid e \circ e \mid \Lambda \alpha : \kappa. e \mid e [\tau] \]

\[ v ::= \text{c} \mid \lambda \alpha : \tau. e \mid \Lambda \alpha : \kappa. e \]
Terms, Types, and Kinds, Oh My

Terms: 
\[ e ::= c | x | \lambda x : \tau. e | e e | \Lambda \alpha :: \kappa. e | e [\tau] \]

\[ v ::= c | \lambda x : \tau. e | \Lambda \alpha :: \kappa. e \]

- atomic values (e.g., \( c \)) and operations (e.g., \( e + e \))
- compound values (e.g., \( (v, v) \)) and operations (e.g., \( e . i \))
- value abstraction and application
- type abstraction and application
- classified by types (but not all terms have a type)

Types: 
\[ \tau ::= \text{int} | \tau \rightarrow \tau | \alpha | \forall \alpha :: \kappa. \tau | \lambda \alpha :: \kappa. \tau | \tau \tau \]

- atomic types (e.g., \( \text{int} \)) classify the terms that evaluate to atomic values
- compound types (e.g., \( \tau \rightarrow \tau \)) classify the terms that evaluate to compound values
- function types \( \tau \rightarrow \tau \) classify the terms that evaluate to value abstractions
- universal types \( \forall \alpha. \tau \) classify the terms that evaluate to type abstractions
- type abstraction and application
- type abstractions do not classify terms, but can be applied to type arguments to form types that do classify terms
- classified by kinds (but not all types have a kind)

Kind Examples

Kinds: 
\[ \kappa ::= * | \kappa \Rightarrow \kappa \]

- kind of proper types \( * \) classify the types (that are the same as the types) that classify terms
- arrow kinds \( \kappa \Rightarrow \kappa \) classify the types (that are the same as the types) that are type abstractions

Terms, Types, and Kinds, Oh My

Types: 
\[ \tau ::= \text{int} | \tau \rightarrow \tau | \alpha | \forall \alpha :: \kappa. \tau | \lambda \alpha :: \kappa. \tau | \tau \tau \]

- atomic types (e.g., \( \text{int} \)) classify the terms that evaluate to atomic values
- compound types (e.g., \( \tau \rightarrow \tau \)) classify the terms that evaluate to compound values
- function types \( \tau \rightarrow \tau \) classify the terms that evaluate to value abstractions
- universal types \( \forall \alpha. \tau \) classify the terms that evaluate to type abstractions
- type abstraction and application
- type abstractions do not classify terms, but can be applied to type arguments to form types that do classify terms
- classified by kinds (but not all types have a kind)
Kind Examples

▶ *
  ▶ the kind of proper types
  ▶ Bool, Bool → Bool, …

▶ * ⇒ *
  ▶ the kind of (unary) type operators
  ▶ List, Maybe, …

Matthew Fluet
CSE-505 2016, Lecture 27
12

Kind Examples

▶ *
  ▶ the kind of proper types
  ▶ Bool, Bool → Bool, …

▶ * ⇒ *
  ▶ the kind of (unary) type operators
  ▶ List, Maybe, …
Kind Examples

- \( \star \)
  - the kind of proper types
  - \( \text{Bool, Bool} \rightarrow \text{Bool, Maybe Bool, Maybe Bool} \rightarrow \text{Maybe Bool, ...} \)
- \( \star \Rightarrow \star \)
  - the kind of (unary) type operators
  - \( \text{List, Maybe, Map Int, Either (List Bool), ...} \)
- \( \star \Rightarrow \star \Rightarrow \star \)
  - the kind of (binary) type operators
  - \( \text{Either, Map, ...} \)
- \( (\star \Rightarrow \star) \Rightarrow \star \)
  - the kind of higher-order type operators
  - taking unary type operators to proper types
  - \( ???, ... \)
- \( (\star \Rightarrow \star) \Rightarrow \star \Rightarrow \star \)
  - the kind of higher-order type operators
  - taking unary type operators to proper types
  - \( ???, ... \)
System Fω: Syntax

\[ e ::= c \mid x \mid \lambda x:\tau.\ e \mid e\ e \mid \Lambda\alpha::\kappa.\ e \mid e[\tau] \]

\[ \nu ::= c \mid \lambda x:\tau.\ e \mid \Lambda\alpha::\kappa.\ e \]

\[ \Gamma ::= \cdot \mid \Gamma, x:\tau \]

\[ \tau ::= \text{int} \mid \tau \to \tau \mid \alpha \mid \forall\alpha::\kappa.\ \tau \mid \lambda\alpha::\kappa.\ \tau \mid \tau \tau \]

\[ \kappa ::= \cdot \mid \kappa, \alpha::\kappa \]

New things:

- Types: type abstraction and type application
- Kinds: the “types” of types
  - \(*\): kind of proper types
  - \(\alpha_a \Rightarrow \alpha_r\): kind of type operators

Should look familiar:

the typing rules of the Simply-Typed Lambda Calculus “one level up”

System Fω: Operational Semantics

Small-step, call-by-value (CBV), left-to-right operational semantics:

\[ e \to_{cbv} e' \]

\[ (\lambda x::\tau.\ e_a) v_a \to_{cbv} e_a[v_a/x] \]

\[ e_f \to_{cbv} e'_f \]

\[ e_f\ e_a \to_{cbv} e'_f\ e'_a \]

\[ \forall\alpha::\kappa_a.\ e_b) \ [\tau_a] \to_{cbv} e_b[\tau_a/\alpha] \]

\[ \forall\alpha::\kappa_a.\ e \ [\tau_a] \to_{cbv} e'_f\ [\tau_a] \]

- Unchanged! All of the new action is at the type-level.

System Fω: Type System, part 1

In the context \(\Delta\) the type \(\tau\) has kind \(\kappa\):

\[ \Delta \vdash \tau :: \kappa \]

\[ \Delta \vdash \text{int} :: * \]

\[ \Delta \vdash \tau_a :: * \]

\[ \Delta \vdash \tau_r :: * \]

\[ \Delta \vdash \tau_a \to \tau_r :: * \]

\[ \Delta(\alpha) = \kappa \]

\[ \Delta, \alpha :: \kappa_a \vdash \tau_r :: * \]

\[ \Delta \vdash \forall\alpha::\kappa_a.\ \tau_r :: * \]

\[ \Delta, \alpha :: \kappa_a \vdash \tau_b :: \kappa_r \]

\[ \Delta \vdash \lambda\alpha::\kappa_a.\ \tau_b :: \kappa_r \]

\[ \Delta \vdash \lambda\alpha::\kappa_a.\ \tau_a :: \kappa_r \]

\[ \Delta \vdash \tau_f :: \kappa_a \Rightarrow \kappa_r \]

\[ \Delta \vdash \lambda\alpha::\kappa_a.\ \tau_f :: \kappa_r \]

\[ \Delta \vdash \tau_f\ \tau_a :: \kappa_r \]

Should look familiar:

the typing rules of the Simply-Typed Lambda Calculus “one level up”
System Fω: Type System, part 3

In the contexts Δ and Γ the expression e has type τ:

\[
\Delta; \Gamma \vdash e : \tau
\]

\[
\Delta; \Gamma \vdash e : \tau,
\quad \Delta; \Gamma \vdash c : \text{int}
\]

\[
\Delta; \Gamma \vdash e f : \tau_a \rightarrow \tau_r,
\quad \Delta; \Gamma \vdash c : \text{int}
\]

\[
\Delta; \Gamma \vdash \lambda x : \tau_a. e_b : \tau_a \rightarrow \tau_r
\]

\[
\Delta; \Gamma \vdash e f \left[ \tau_a \right] : \tau_r[\tau_a/\alpha]
\]

\[
\Delta; \Gamma \vdash e : \tau \equiv \tau',
\quad \Delta; \Gamma \vdash e : \tau
\]

\[
\Delta; \Gamma \vdash e : \tau \equiv \tau',
\quad \Delta; \Gamma \vdash e : \tau
\]

\[
\Delta; \Gamma \vdash e \left[ \tau_a \right] : \tau_r[\tau_a/\alpha]
\]

\[
\Delta; \Gamma \vdash e : \tau \equiv \tau',
\quad \Delta; \Gamma \vdash e : \tau
\]

\[
\Delta; \Gamma \vdash e \left[ \tau_a \right] : \tau_r[\tau_a/\alpha]
\]

\[
\Delta; \Gamma \vdash e : \tau \equiv \tau',
\quad \Delta; \Gamma \vdash e : \tau
\]

\[
\Delta; \Gamma \vdash e \left[ \tau_a \right] : \tau_r[\tau_a/\alpha]
\]

\[
\Delta; \Gamma \vdash e : \tau \equiv \tau',
\quad \Delta; \Gamma \vdash e : \tau
\]

\[
\Delta; \Gamma \vdash e \left[ \tau_a \right] : \tau_r[\tau_a/\alpha]
\]

\[
\Delta; \Gamma \vdash e : \tau \equiv \tau',
\quad \Delta; \Gamma \vdash e : \tau
\]

\[
\Delta; \Gamma \vdash e \left[ \tau_a \right] : \tau_r[\tau_a/\alpha]
\]

\[
\Delta; \Gamma \vdash e : \tau \equiv \tau',
\quad \Delta; \Gamma \vdash e : \tau
\]

\[
\Delta; \Gamma \vdash e \left[ \tau_a \right] : \tau_r[\tau_a/\alpha]
\]

\[
\Delta; \Gamma \vdash e : \tau \equiv \tau',
\quad \Delta; \Gamma \vdash e : \tau
\]

\[
\Delta; \Gamma \vdash e \left[ \tau_a \right] : \tau_r[\tau_a/\alpha]
\]

\[
\Delta; \Gamma \vdash e : \tau \equiv \tau',
\quad \Delta; \Gamma \vdash e : \tau
\]

\[
\Delta; \Gamma \vdash e \left[ \tau_a \right] : \tau_r[\tau_a/\alpha]
\]

\[
\Delta; \Gamma \vdash e : \tau \equiv \tau',
\quad \Delta; \Gamma \vdash e : \tau
\]

\[
\Delta; \Gamma \vdash e \left[ \tau_a \right] : \tau_r[\tau_a/\alpha]
\]
Polymorphic List Library with higher-order $\exists$

List library is an existential package:

\[
\text{pack}(\lambda \alpha :: \star. \mu \xi :: \star. \text{unit} + (\alpha \ast \xi), \text{list_library})
\]
as $\exists L :: \star \Rightarrow \star. \{\text{empty} : \forall \alpha :: \star. L \alpha;$
\[
\text{cons} : \forall \alpha :: \star. \alpha \rightarrow L \alpha \rightarrow L \alpha;
\]
\[
\text{unlist} : \forall \alpha :: \star. L \alpha \rightarrow \text{unit} + (\alpha \ast L \alpha);
\]
\[
\text{map} : \forall \alpha :: \star. \forall \beta :: \star. (\alpha \rightarrow \beta) \rightarrow L \alpha \rightarrow L \beta;
\]
\[
\ldots\}
\]

The witness type operator is poly.lists: $\lambda \alpha :: \star. \mu \xi :: \star. \text{unit} + (\alpha \ast \xi)$.

The existential type operator variable $L$ represents poly. lists.

List operations are polymorphic in element type.

The map function only allows mapping $\alpha$ lists to $\beta$ lists.

Other Kinds of Kinds

Kinding systems for checking and tracking properties of type expressions:

- Record kinds
  - records at the type-level; define systems of mutually recursive types
- Polymorphic kinds
  - kind abstraction and application in types; System F “one level up”
- Dependent kinds
  - dependent types “one level up”
- Row kinds
  - describe “pieces” of record types for record polymorphism
- Power kinds
  - alternative presentation of subtyping
- Singleton kinds
  - formalize module systems with type sharing

Metatheory

System $F_\omega$ is type safe.

- Preservation:
  Induction on typing derivation, using substitution lemmas:
  - Term Substitution:
    - if $\Delta_1, \Delta_2; \Gamma_1, x :: \tau_\alpha, \Gamma_2 \vdash e_1 : \tau_\alpha$ and $\Delta_1; \Gamma_1 \vdash e_2 : \tau_x$, then $\Delta_1, \Delta_2; \Gamma_1, \Gamma_2 \vdash e_1[e_2/x] :: \tau$.
  - Type Substitution:
    - if $\Delta_1, \alpha :: \kappa_\alpha, \Delta_2 \vdash \tau_1 :: \kappa$ and $\Delta_1 \vdash \tau_2 :: \kappa_\alpha$, then $\Delta_1, \Delta_2 \vdash \tau_1[\tau_2/\alpha] :: \kappa$.
  - Type Substitution:
    - if $\tau_1 \equiv \tau_2$, then $\tau_1[\tau/\alpha] \equiv \tau_2[\tau/\alpha]$.
  - Type Substitution:
    - if $\Delta_1, \alpha :: \kappa_\alpha, \Delta_2; \Gamma_1, \Gamma_2 \vdash e_1 : \tau$ and $\Delta_1 \vdash \tau_2 :: \kappa_\alpha$, then $\Delta_1, \Delta_2; \Gamma_1, \Gamma_2[\tau_2/\alpha] \vdash e_1[\tau_2/\alpha] :: \tau$.
  - All straightforward inductions, using various weakening and exchange lemmas.
Matthew Fluet

Definitional Equivalence and Parallel Reduction

Key properties:

- Transitive and symmetric closure of parallel reduction and type equivalence coincide:
  - $\tau \Leftrightarrow^* \tau'$ iff $\tau \equiv \tau'$

Metatheory

System $F_\omega$ is type safe.

- Progress:
  - Induction on typing derivation, using canonical form lemmas:
    - If $\cdot; \vdash v : \text{int}$, then $v = c$.
    - If $\cdot; \vdash v : \tau_a \rightarrow \tau_r$, then $v = \lambda x: \tau_a. \ e_b$.
    - If $\cdot; \vdash v : \forall \alpha::\kappa_a. \ \tau_r$, then $v = \Delta \alpha::\kappa_a. \ e_b$.
  - Complicated by typing derivations that end with:
    
    $\Delta; \Gamma \vdash e : \tau \quad \tau \equiv \tau' \quad \Delta; \Gamma \vdash \tau' :: * \quad \tau' \equiv \tau' :: *$

    (just like with subtyping and subsumption).

Definitional Equivalence and Parallel Reduction

Parallel Reduction of $\tau$ to $\tau'$:

$\tau \Rightarrow \tau'$

$\tau \Rightarrow \tau$

$\tau_a1 \Rightarrow \tau_a2 \quad \tau_r1 \Rightarrow \tau_r2$

$\tau_a1 \Rightarrow \tau_r1 \Rightarrow \tau_a2 \Rightarrow \tau_r2$

$\forall \alpha::\kappa_a. \ \tau_r1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_r2$

$\tau_r1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_r1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_r2$

$\lambda \alpha::\kappa_a. \ \tau_b1 \Rightarrow \lambda \alpha::\kappa_a. \ \tau_b2$

$\lambda \alpha::\kappa_a. \ \tau_b2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_b2$

$\forall \alpha::\kappa_a. \ \tau_f1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f2$

$\forall \alpha::\kappa_a. \ \tau_f2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1$

$\forall \alpha::\kappa_a. \ \tau_a1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_a2$

$\forall \alpha::\kappa_a. \ \tau_a2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_a1$

$\forall \alpha::\kappa_a. \ \tau_f1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f2$

$\forall \alpha::\kappa_a. \ \tau_f2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1$

$\tau_f1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f2$

$\forall \alpha::\kappa_a. \ \tau_a2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_a1$

$\forall \alpha::\kappa_a. \ \tau_a1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_a2$

$\forall \alpha::\kappa_a. \ \tau_f2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1$

$\forall \alpha::\kappa_a. \ \tau_f1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f2$

$\forall \alpha::\kappa_a. \ \tau_f2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1$

$\forall \alpha::\kappa_a. \ \tau_a1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_a2$

$\forall \alpha::\kappa_a. \ \tau_a2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_a1$

$\forall \alpha::\kappa_a. \ \tau_f1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f2$

$\forall \alpha::\kappa_a. \ \tau_f2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1$

$\forall \alpha::\kappa_a. \ \tau_f2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1$

$\forall \alpha::\kappa_a. \ \tau_f1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f2$

$\forall \alpha::\kappa_a. \ \tau_f2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1$

$\forall \alpha::\kappa_a. \ \tau_f1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f2$

$\forall \alpha::\kappa_a. \ \tau_f2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1$

$\forall \alpha::\kappa_a. \ \tau_a1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_a2$

$\forall \alpha::\kappa_a. \ \tau_a2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_a1$

$\forall \alpha::\kappa_a. \ \tau_f1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f2$

$\forall \alpha::\kappa_a. \ \tau_f2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1$

$\forall \alpha::\kappa_a. \ \tau_f2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1$

$\forall \alpha::\kappa_a. \ \tau_f1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f2$

$\forall \alpha::\kappa_a. \ \tau_f2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1$

$\forall \alpha::\kappa_a. \ \tau_f1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f2$

$\forall \alpha::\kappa_a. \ \tau_f2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1$

$\forall \alpha::\kappa_a. \ \tau_f1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f2$

$\forall \alpha::\kappa_a. \ \tau_f2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1$

$\forall \alpha::\kappa_a. \ \tau_f1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f2$

$\forall \alpha::\kappa_a. \ \tau_f2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1$

$\forall \alpha::\kappa_a. \ \tau_f1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f2$

$\forall \alpha::\kappa_a. \ \tau_f2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1$

$\forall \alpha::\kappa_a. \ \tau_f1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f2$

$\forall \alpha::\kappa_a. \ \tau_f2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1$

$\forall \alpha::\kappa_a. \ \tau_f1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f2$

$\forall \alpha::\kappa_a. \ \tau_f2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1$

$\forall \alpha::\kappa_a. \ \tau_f1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f2$

$\forall \alpha::\kappa_a. \ \tau_f2 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f1$

$\forall \alpha::\kappa_a. \ \tau_f1 \Rightarrow \forall \alpha::\kappa_a. \ \tau_f2$
Definitional Equivalence and Parallel Reduction

Key properties:
- Transitive and symmetric closure of parallel reduction and type equivalence coincide:
  - $\tau \iff^* \tau'$ iff $\tau \equiv \tau'$
- Parallel reduction has the Church-Rosser property:
  - If $\tau \Rightarrow^* \tau_1$ and $\tau \Rightarrow^* \tau_2$, then there exists $\tau'$ such that $\tau_1 \Rightarrow^* \tau'$ and $\tau_2 \Rightarrow^* \tau'$
- Equivalent types share a common reduct:
  - If $\tau_1 \equiv \tau_2$, then there exists $\tau'$ such that $\tau_1 \Rightarrow^* \tau'$ and $\tau_2 \Rightarrow^* \tau'$

Reduction preserves shapes:
- If $\text{int} \Rightarrow^* \tau'$, then $\tau' = \text{int}$
- If $\tau_a \rightarrow \tau_r \Rightarrow^* \tau'_r$, then $\tau'_r = \tau'_a \rightarrow \tau'_r$ and $\tau_a \Rightarrow^* \tau'_a$ and $\tau_r \Rightarrow^* \tau'_r$
- If $\forall \alpha :: \kappa_a, \tau_r \Rightarrow^* \tau'_r$, then $\tau'_r = \forall \alpha :: \kappa_a, \tau'_r$ and $\tau_r \Rightarrow^* \tau'_r$

Canonical Forms

If $\cdot ; \cdot \vdash v : \tau_a \rightarrow \tau_r$, then $v = \lambda x : \tau_a. e_b$.
Proof:
By cases on the form of $v$:
Canonical Forms

If \( \cdot \vdash \, v : \tau_a \to \tau_r \), then \( v = \lambda x: \tau_a. \, e_b \).

Proof:
By cases on the form of \( v \):

\[ v = \lambda x: \tau_a. \, e_b. \]

We have that \( v = \lambda x: \tau_a. \, e_b. \)

\[ v = \Lambda \alpha:: \kappa_a. \, e_b. \]

Derivation of \( \cdot \vdash \, v : \tau_a \to \tau_r \) must be of the form:

\[ \vdash \Delta \vdash \tau : \kappa \]

Therefore, we can construct the derivation \( \tau \equiv \tau_{\alpha} \to \tau_r \).

We can find a common reduct: \( \tau \Rightarrow^* \tau^f \) and \( \tau_{\alpha} \to \tau_r \Rightarrow^* \tau_{\alpha}^f \).

Reduction preserves shape: \( \tau \Rightarrow^* \tau^f \) implies \( \tau^f = \tau_{\alpha} \to \tau_r^f \).

But, \( \tau^f = \tau_{\alpha} \to \tau_r^f \) and \( \tau^f = \tau_{\alpha}^f \to \tau_r^f \) is a contradiction.

Metatheory

System \( F_{\omega} \) is type safe.

Where was the \( \Delta \vdash \tau : \kappa \) judgement used in the proof?
Metatheory

System $F_\omega$ is type safe.

Where was the $\Delta \vdash \tau :: \kappa$ judgement used in the proof?
In Type Substitution lemmas, but only in an inessential way.

After weeks of thinking about type systems, kinding seems natural;
but kinding is not required for type safety!
This language is type safe.

Check that free type variables of \( \tau \) are in \( \Delta \), but nothing else.
This language is type safe.

- **Preservation:**
  Induction on typing derivation, using substitution lemmas:
  - Term Substitution:
    if $\Delta_1, \Delta_2; \Gamma_1, x : \tau_x, \Gamma_2 \vdash e_1 : \tau$ and $\Delta_1; \Gamma_1 \vdash e_2 : \tau_x$, then $\Delta_1, \Delta_2; \Gamma_1, \Gamma_2 \vdash e_1[e_2/x] : \tau$.
  - Type Substitution:
    if $\Delta_1, \alpha, \Delta_2 \vdash \tau_1 :: ✓$ and $\Delta_1 \vdash \tau_2 :: ✓$, then $\Delta_1, \Delta_2 \vdash \tau_1[\tau_2/\alpha] :: ✓$.
  - Type Substitution:
    if $\tau_1 \equiv \tau_2$, then $\tau_1[\tau/\alpha] \equiv \tau_2[\tau/\alpha]$.
  - Type Substitution:
    if $\Delta_1, \alpha, \Delta_2; \Gamma_1, \Gamma_2 \vdash e_1 : \tau$ and $\Delta_1 \vdash \tau_2 :: ✓$, then $\Delta_1, \Delta_2; \Gamma_1, \Gamma_2[\tau_2/\alpha] \vdash e_1[\tau_2/\alpha] : \tau$.
  - All straightforward inductions, using various weakening and exchange lemmas.

- **Progress:**
  Induction on typing derivation, using canonical form lemmas:
  - If $\cdot; \cdot \vdash v : \texttt{int}$, then $v = c$.
  - If $\cdot; \cdot \vdash v : \tau_a \rightarrow \tau_r$, then $v = \lambda x : \tau_a. e_b$.
  - If $\cdot; \cdot \vdash v : \forall \alpha. \tau_r$, then $v = \Lambda \alpha. e_b$.
  - Using parallel reduction relation.

**Why Kinds?**

Why aren’t kinds required for type safety?

Recall statement of type safety:

If $\cdot; \cdot \vdash e : \tau$, then $e$ does not get stuck.
Why Kinds?

Why aren’t kinds required for type safety?

Recall statement of type safety:

If $\cdot; \cdot \vdash e : \tau$, then $e$ does not get stuck.

The typing derivation $\cdot; \cdot \vdash e : \tau$
includes definitional-equivalence sub-derivations $\tau \equiv \tau'$,
which are explicit evidence that $\tau$ and $\tau'$ are the same.

▶ E.g., to show that the “natural” type of the function expression
in an application is equivalent to an arrow type:

\[
\begin{align*}
\Delta; \Gamma \vdash e_f : \tau_f & \quad \tau_f \equiv \tau_a \rightarrow \tau_r \\
\Delta; \Gamma \vdash e : \tau_a & \\
\Delta; \Gamma \vdash e_f e_a : \tau_r
\end{align*}
\]

Definitional equivalence ($\tau \equiv \tau'$) and parallel reduction ($\tau \Rightarrow \tau'$)
do not require well-kinded types (although they preserve the kinds of well-kinded types).

▶ E.g., $(\lambda \alpha. \alpha \rightarrow \alpha) (\text{int} \text{ int}) \equiv (\text{int} \text{ int}) \rightarrow (\text{int} \text{ int})$

Why Kinds?

Why aren’t kinds required for type safety?

Recall statement of type safety:

If $\cdot; \cdot \vdash e : \tau$, then $e$ does not get stuck.

The typing derivation $\cdot; \cdot \vdash e : \tau$
includes definitional-equivalence sub-derivations $\tau \equiv \tau'$,
which are explicit evidence that $\tau$ and $\tau'$ are the same.

Definitional equivalence ($\tau \equiv \tau'$) and parallel reduction ($\tau \Rightarrow \tau'$)
do not require well-kinded types (although they preserve the kinds of well-kinded types).

Type (and kind) erasure means that “wrong/bad/meaningless” types
do not affect run-time behavior.

▶ Ill-kinded types can’t make well-typed terms get stuck.
Why Kinds?

Kinds aren't for *type safety*:
- Because a typing derivation (even with ill-kinded types), carries enough evidence to guarantee that expressions don't get stuck.

Kinds are for *type checking*:
- Because programmers write programs, not typing derivations.
- Because type checkers are algorithms.

Recall the statement of type checking:

Given \( \Delta, \Gamma, \) and \( e \), does there exist \( \tau \) such that \( \Delta; \Gamma \vdash e : \tau \).

Two issues:
- \( \Delta; \Gamma \vdash e : \tau \equiv \tau' \ \Delta \vdash \tau' :: \star \) is a non-syntax-directed rule
- \( \tau \equiv \tau' \) is a non-syntax-directed relation

One non-issue:
- \( \Delta \vdash \tau :: \kappa \) is a syntax-directed relation (STLC “one level up”)

Matthew Fluet CSE-505 2016, Lecture 27
Type Checking for System F\(\omega\)

Remove non-syntax-directed rules and relations:
\[
\Delta; \Gamma \vdash e : \tau
\]

\[
\begin{align*}
\Delta; \Gamma \vdash e : \text{int} & \quad \Delta; \Gamma \vdash x : \tau \\
\Delta \vdash \tau_a :: \ast & \quad \Delta; \Gamma, x : \tau_a \vdash e_b : \tau_r \\
\Delta; \Gamma \vdash \lambda x : \tau_a. \ e_b : \tau_a \to \tau_r
\end{align*}
\]

Metatheory for kind system:
- Well-kinded types don’t get stuck.
  - If \(\Delta \vdash \tau :: \kappa\) and \(\tau \Rightarrow^* \tau'\),
    then either \(\tau'\) is in (weak-head) normal form (i.e., a type-level “value”)
    or \(\tau' \Rightarrow \tau''\).
  - Proofs by Progress and Preservation on kinding and parallel reduction derivations.

Type Checking for System F\(\omega\)

Kinds are for type checking.

Given \(\Delta\), \(\Gamma\), and \(e\), does there exist \(\tau\) such that \(\Delta; \Gamma \vdash e : \tau\).

Proofs by Progress and Preservation on kinding and parallel reduction derivations.

But, irrelevant for type checking of expressions.

If \(\tau_f \Rightarrow^\ast \tau'_f\) “gets stuck” at a type \(\tau'_f\) that is not an arrow type, then the application typing rule does not apply
and a typing derivation does not exist.
Type Checking for System $\text{F}_\omega$

Kinds are for type checking.

Given $\Delta$, $\Gamma$, and $e$, does there exist $\tau$ such that $\Delta; \Gamma \vdash e : \tau$.

Metatheory for kind system:

- Well-kinded types don’t get stuck.
  - If $\Delta \vdash \tau :: \kappa$ and $\tau \Rightarrow^* \tau'$, then either $\tau'$ is in (weak-head) normal form (i.e., a type-level “value”) or $\tau' \Rightarrow \tau''$.
  - But, irrelevant for type checking of expressions.
- Well-kinded types terminate.
  - If $\Delta \vdash \tau :: \kappa$, then there exists $\tau'$ such that $\tau \Rightarrow^\Psi \tau'$.
  - Proof is similar to that of termination of STLC.

Type checking for System $\text{F}_\omega$ is decidable.

Going Further

This is just the tip of an iceberg.

- Pure type systems
  - Why stop at three levels of expressions (terms, types, and kinds)?
  - Allow abstraction and application at the level of kinds, and introduce sorts to classify kinds.
  - Why stop at four levels of expressions?
  - For programming languages, however, three levels have proved sufficient.

Metatheory for kind system:

- Well-kinded types don’t get stuck.
  - If $\Delta \vdash \tau :: \kappa$ and $\tau \Rightarrow^* \tau'$, then either $\tau'$ is in (weak-head) normal form (i.e., a type-level "value") or $\tau' \Rightarrow \tau''$.
  - But, irrelevant for type checking of expressions.
- Well-kinded types terminate.
  - If $\Delta \vdash \tau :: \kappa$, then there exists $\tau'$ such that $\tau \Rightarrow^\Psi \tau'$.

Type Checking for System $\text{F}_\omega$

Kinds are for type checking.

Given $\Delta$, $\Gamma$, and $e$, does there exist $\tau$ such that $\Delta; \Gamma \vdash e : \tau$.