EDAP15: Program Analysis

MONOMORPHIC TYPE ANALYSIS

Christoph Reichenbach

Basic Formal Notation

- Tuples:
  - Notation: $\langle a \rangle$, $\langle a, b \rangle$ (pair), $\langle a, c, d \rangle$ (triple)
  - Fixed-length (unlike list)
  - Group items, analogous to (read-only) record/object
- Sets:

$\emptyset = \{\}$	(the empty set)
$\{1\}$	(*singleton* set containing precisely the number 1)
$\{2, 3\}$	(Set with two elements)
$\mathbb{Z}$	(The (infinite) set of integers)
$\mathbb{R}$	(The (infinite) set of real numbers)

Basic operations on sets

$x \in S$	Is x contained in S?	True: $1 \in \{1\}$ and $1 \in \mathbb{Z}$ False: $2 \in \{1\}$ or $\pi \in \mathbb{R}$
$x \notin S$	Is x NOT containd in S?	
$A \cup B$	Set union	$\{1\} \cup \{2\} = \{1, 2\}$ $\{1, 3\} \cup \{2, 3\} = \{1, 2, 3\}$
$A \cap B$	Set intersection	$\{1\} \cap \{2\} = \emptyset$ $\{1, 3\} \cap \{2, 3\} = \{3\}$
$A \subseteq B$	Subset relationship	True: $\emptyset \subseteq \{1\}$ and $\mathbb{Z} \subseteq \mathbb{R}$ False: $\{2\} \subseteq \{1\}$
$A \times B$	Product set	$\{1, 2\} \times \{3, 4\} \times \{5, 6\}$ $= \{\langle 1, 3\rangle, \langle 1, 4\rangle, \langle 2, 3\rangle, \langle 2, 4\rangle\}$

Relations

A relation R of arity n is a set of tuples of the form

$$R = \{ \ \langle v_1^1, v_2^1, \ldots, v_n^1 \rangle \\ \vdots \\ \langle v_1^k, v_2^k, \ldots, v_n^k \rangle \ \}$$

- Notation:

$$R(x_1, \ldots, x_n) \iff \langle x_1, \ldots, x_n \rangle \in R$$

- Example: the less-than-or-equals relation over integers:

$$(\leq) \subseteq \mathbb{Z} \times \mathbb{Z}$$

$\langle 1, 2 \rangle$ $\langle 2, 2 \rangle$

$\langle 3, 0 \rangle \notin (\leq)$

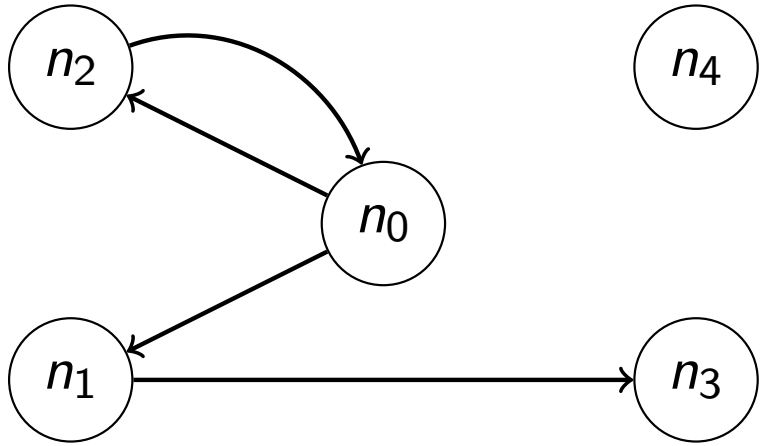
- Relations of arity 2 are called *binary* relations:
  - Notation:

$$R(x, y) \iff x \ R \ y$$

Graphs

A (directed) graph $\mathcal{G}$ is a tuple $\mathcal{G} = \langle \mathcal{N}, \mathcal{E} \rangle$, where:

- $\mathcal{N}$ is the set of *nodes* of $\mathcal{G}$
- $\mathcal{E} \subseteq \mathcal{N} \times \mathcal{N}$ is the set of *edges* of $\mathcal{G}$
- Often: Add function $f : \mathcal{E} \to X$ to *label* edges



$\mathcal{N} = \{n_0, n_1, n_2, n_3, n_4\}$

$\mathcal{E} = \{\langle n_0, n_1 \rangle, \langle n_0, n_2 \rangle, \langle n_1, n_3 \rangle, \langle n_2, n_0 \rangle\}$

Summary

- **Tuples** group a fixed number of items
- **Sets** represent a (possibly infinite) number of distinct elements
  - We use them e.g. to represent possible analysis results
- **Relations** are sets of equal-sized tuples
  - We mostly use them implicitly
  - Similar to database tables, but:
    - No duplicate rows
    - No row order
- **(Directed) Graphs** represent *nodes* and *edges* between them
  - Optional *labels* on edges possible
  - We use them e.g. for program dependencies

Types

Java	Haskell	ML
`int v;`	`v :: Int`	`val v : int`

- Framework for classifying parts of programs by:
  - Which set they may be drawn from, and/or
  - What behaviour they exhibit
- *Type analysis* deals with:
  - *Checking types*: Do the types agree?
  - *Inferring types*: Given part of a program, what is its type?
- We focus on *static type analysis*

Types and Programs: Two Lanugages

Language $\mathcal{V}$:

$$\begin{array}{lcl} \mathit{val} & ::= & \mathit{nat} \\ & \mid & \mathsf{true} \mid \mathsf{false} \end{array}$$

Language $\mathbb{T}_{\mathcal{V}}$:

$$\begin{array}{lcl} \mathit{type} & ::= & \textsc{Int} \\ & \mid & \textsc{Bool} \end{array}$$

- For program analysis, best to consider types and programs *separate* languages
  - Target language's type system may not match our needs
  - Language $\mathcal{V}$ entirely lacks type system
- Abstract over $\mathcal{V}$ with $\mathbb{T}_{\mathcal{V}}$:

$$\mathit{23} : \textsc{Int} \qquad\qquad \mathsf{true} : \textsc{Bool}$$

- From that perspective, "has-type-of" is a binary relation:

$$(:) \subseteq \mathcal{V} \times \mathbb{T}_{\mathcal{V}}$$

Uses of Type Analysis

- Types abstractly model program behaviour
- "Traditionally":
  - Set of possible computational results
  - Set of possible behaviours of computational result
- We can model other behaviour as types:
  - Uncaught exceptions
  - Use of shared memory regions
  - Other side effects ← might also need types for statements
  - Dependencies
  - Race conditions in concurrent memory access

  ...

Applying Type Systems

x : Bool
x : Int

Given program p: analyse $p : \tau$

Type Checking

- Assume τ is *given*
- Test: **Is $p : \tau$ true?**
- Can *use* type inference

Type Inference

- Assume τ is *not given*
- Find all τ s.th. $p : \tau$
  - None/Multiple: *Type Error*

Program Analysis Designer's View

int f (@NonNull Object o) {

- *Checking* τ requires specification
- Examples:
  - User spec: "no exceptions"
  - Language spec: "no side effects allowed here"
- *Inferring* τ can sensibly yield multiple results
  - Zero/many properties of interest
  - Example: τ describes type of exception that might be raised

Summary

- Types abstractly *model* some aspect of a program
- For a given analysis, the language of *types* and *programs* might be distinct

  - set of throwable exceptions
  - number of objects allocated
  - whether there are side effects

- Type analysis examines:
  - **Type Checking** Does this program have some specific type?
  - **Type Analysis** Which types can this program have?
- Standard notation: the binary **typing relation** (:) relates programs p and their types τ:

$$\boxed{p : \tau}$$

A Simple Language: IGA

e_1 if cond else e_2

cond ? e_1 : e_2

$$
\begin{array}{lcl}
\mathit{expr} & ::= & \langle \mathit{val} \rangle \\
 & | & \langle \mathit{expr} \rangle \ \mathrm{plus} \ \langle \mathit{expr} \rangle \\
 & | & \langle \mathit{expr} \rangle \ >= \ \langle \mathit{expr} \rangle \\
 & | & \mathrm{if} \ \langle \mathit{expr} \rangle \ \mathrm{then} \ \langle \mathit{expr} \rangle \ \mathrm{else} \ \langle \mathit{expr} \rangle \\
\mathit{val} & ::= & \mathit{nat} \\
 & | & \mathrm{true} \ | \ \mathrm{false} \\
\mathit{nat} & ::= & 0 \ | \ 1 \ | \ 2 \ | \ 3 \ | \ 4 \ | \ \ldots
\end{array}
$$

- Semantics mostly straightforward:
- plus operates only on *nat*

A Simple Language: IGA

$$
\begin{array}{lcl}
\mathit{expr} & ::= & \langle \mathit{val} \rangle \\
 & | & \langle \mathit{expr} \rangle \ \mathsf{plus} \ \langle \mathit{expr} \rangle \\
 & | & \langle \mathit{expr} \rangle \ >= \ \langle \mathit{expr} \rangle \\
 & | & \mathsf{if} \ \langle \mathit{expr} \rangle \ \mathsf{then} \ \langle \mathit{expr} \rangle \ \mathsf{else} \ \langle \mathit{expr} \rangle \\
 & & \\
\mathit{val} & ::= & \mathit{nat} \\
 & | & \mathsf{true} \ | \ \mathsf{false} \\
 & & \\
\mathit{nat} & ::= & 0 \ | \ 1 \ | \ 2 \ | \ 3 \ | \ 4 \ | \ \ldots
\end{array}
$$

- Semantics mostly straightforward:
- plus operates only on *nat*
- $>=$ requires *nat* arguments and returns true or false

A Simple Language: IGA

$$
\begin{array}{lcl}
\mathit{expr} & ::= & \langle \mathit{val} \rangle \\
 & | & \langle \mathit{expr} \rangle \ \text{plus} \ \langle \mathit{expr} \rangle \\
 & | & \langle \mathit{expr} \rangle \ >= \ \langle \mathit{expr} \rangle \\
 & | & \text{if} \ \langle \mathit{expr} \rangle \ \text{then} \ \langle \mathit{expr} \rangle \ \text{else} \ \langle \mathit{expr} \rangle \\
 & & \\
\mathit{val} & ::= & \mathit{nat} \\
 & | & \text{true} \ | \ \text{false} \\
 & & \\
\mathit{nat} & ::= & 0 \ | \ 1 \ | \ 2 \ | \ 3 \ | \ 4 \ | \ \ldots
\end{array}
$$

- Semantics mostly straightforward:
- plus operates only on *nat*
- $>=$ requires *nat* arguments and returns true or false
- **if** e_1 **then** e_2 **else** e_3:
  - If e_1 evaluates to true: computes e_2
  - If e_1 evaluates to false: computes e_3

The Typing Relation

- We the set of types of IGA, $\mathbb{T}_{iga} = \{\textsc{Bool}, \textsc{Int}\}$:
  - $\textsc{Bool}$: Type of booleans (true, false)
  - $\textsc{Int}$: Type of natural numbers (0, 1, 2, ...)
- We can now type values:

$$\begin{array}{lcl} \text{true} & : & \textsc{Bool} \\ 23 & : & \textsc{Int} \end{array}$$

- Correspondibly (:) is a binary relation:

$$(:) \subseteq \mathit{val} \times \mathbb{T}_{iga}$$

Types for Values

- To analyse all of IGA, we extend (:) to expressions:

$$(:) \subseteq \mathit{expr} \times \mathbb{T}_{\mathit{iga}}$$

- We want to type e.g.:

$$\underline{\text{39 plus 3}} \quad : \quad \underline{\textsc{Int}}$$

Types for Values

- To analyse all of IGA, we extend (:) to expressions:

$$(:) \subseteq \mathit{expr} \times \mathbb{T}_{\mathit{iga}}$$

- We want to type e.g.:

$$\text{39 plus 3} \quad : \quad \textsc{Int}$$

For clarity, we will write this formally

Types for Expressions

$$\frac{}{\mathsf{true} : \textsc{Bool}}\ (\textit{t-true}) \qquad \frac{}{\mathsf{false} : \textsc{Bool}}\ (\textit{t-false})$$

Types for Expressions

$$\frac{}{\mathsf{true} : \textsc{Bool}}\ (\textit{t-true}) \qquad \frac{}{\mathsf{false} : \textsc{Bool}}\ (\textit{t-false}) \qquad \frac{v \in \mathit{nat}}{v : \textsc{Int}}\ (\textit{t-nat})$$

Conditional Typing Rules

$$\frac{v \in nat}{v : \textsc{Int}}$$

Conditional Typing Rules

$$\frac{v \in nat}{\underbrace{v}_{\text{Program}} : \underbrace{\textsc{Int}}_{\text{Type}}}$$

Conditional Typing Rules

$$\frac{v \in nat}{\underbrace{v}_{\text{Program}} : \underbrace{\textsc{Int}}_{\text{Type}}}$$

Premise / Condition

Conclusion

If $v \in nat$ holds, then so does $v : \textsc{Int}$

Conditional Typing Rules

$$\frac{v \in nat}{v : \textsc{Int}}$$

Premise / Condition

Conclusion

Program

Type

If $v \in nat$ holds, then so does $v : \textsc{Int}$

- v is a *Metavariable*
- We can replace v by *anything*

Conditional Typing Rules

$$\frac{v \in nat}{v : \textsc{Int}}$$

Premise / Condition

Conclusion

Program

Type

If $v \in nat$ holds, then so does $v : \textsc{Int}$

- v is a *Metavariable*
- We can replace v by *anything*
  - One restriction: we must do so *everywhere in the rule at once*

$\Rightarrow$ "*Substitution*"

Conditional Typing Rules

$$\frac{\pi \in \mathit{nat}}{\underbrace{\pi}_{\text{Program}} : \underbrace{\textsc{Int}}_{\text{Type}}}$$

If $\pi \in \mathit{nat}$ holds, then so does $\pi : \textsc{Int}$

- v is a *Metavariable*
- We can replace v by *anything*
  - One restriction: we must do so *everywhere in the rule at once*

$\Rightarrow$ "*Substitution*"

Conditional Typing Rules

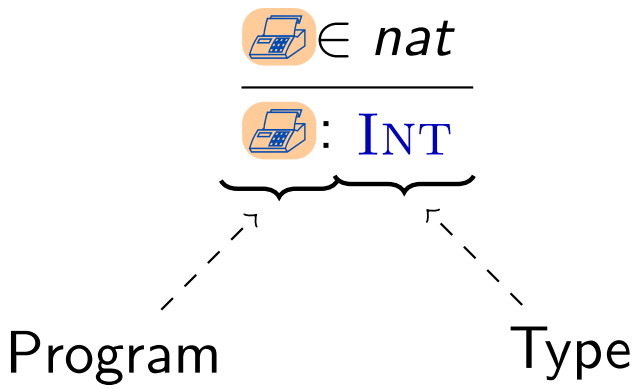
$$\frac{\pi \in \mathit{nat}}{\underbrace{\pi}_{\text{Program}} : \underbrace{\textsc{Int}}_{\text{Type}}}$$

If $\pi \in \mathit{nat}$ holds, then so does $\pi : \textsc{Int}$

- v is a *Metavariable*
- We can replace v by *anything*
  - One restriction: we must do so *everywhere in the rule at once*

$\Rightarrow$ "*Substitution*"

Conditional Typing Rules

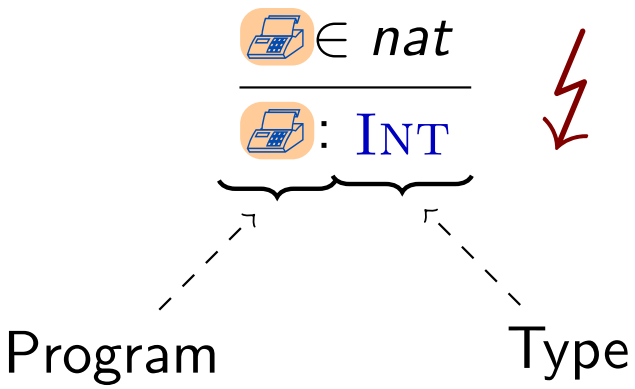


If  $\in$ *nat* holds, then so does  : INT

- v is a *Metavariable*
- We can replace v by *anything*
  - One restriction: we must do so *everywhere in the rule at once*

$\Rightarrow$ "*Substitution*"

Conditional Typing Rules



If  $\in$ *nat* holds, then so does  : INT

- v is a *Metavariable*
- We can replace v by *anything*
  - One restriction: we must do so *everywhere in the rule at once*

$\Rightarrow$ "*Substitution*"

Conditional Typing Rules

$$\frac{42 \in \mathit{nat}}{\underbrace{42}_{\text{Program}} : \underbrace{\textsc{Int}}_{\text{Type}}}$$

If $42 \in \mathit{nat}$ holds, then so does $42 : \textsc{Int}$

- v is a *Metavariable*
- We can replace v by *anything*
  - One restriction: we must do so *everywhere in the rule at once*

$\Rightarrow$ "*Substitution*"

Conditional Typing Rules

$$\frac{42 \in \mathit{nat}}{\underbrace{42}_{\text{Program}} : \underbrace{\textsc{Int}}_{\text{Type}}} \checkmark$$

If $42 \in \mathit{nat}$ holds, then so does $42 : \textsc{Int}$

- v is a *Metavariable*
- We can replace v by *anything*
  - One restriction: we must do so *everywhere in the rule at once*

$\Rightarrow$ "*Substitution*"

Types for Expressions

$$\frac{}{\text{true} : \textsc{Bool}}\ (t\text{-}true) \qquad \frac{}{\text{false} : \textsc{Bool}}\ (t\text{-}false) \qquad \frac{v \in nat}{v : \textsc{Int}}\ (t\text{-}nat)$$

false : Bool

Types for Expressions

$$\frac{}{\mathsf{true} : \textsc{Bool}}\ (\textit{t-true}) \qquad \frac{}{\mathsf{false} : \textsc{Bool}}\ (\textit{t-false}) \qquad \frac{v \in \textit{nat}}{v : \textsc{Int}}\ (\textit{t-nat})$$

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1\ \mathsf{plus}\ e_2 : \textsc{Int}}\ (\textit{t-plus})$$

Recursive Typing Rules

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}} \; (\textit{t-plus})$$

$$\frac{v \in \textit{nat}}{v : \textsc{Int}} \; (\textit{t-nat})$$

$$\underline{1 \text{ plus } 2 \text{ plus } 3} : \textsc{Int}$$

Recursive Typing Rules

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}} \; (\textit{t-plus})$$

$$\frac{v \in \textit{nat}}{v : \textsc{Int}} \; (\textit{t-nat})$$

$$\Downarrow$$

$$\boxed{\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}} \; (\textit{t-plus})}$$

$$1 \text{ plus } 2 \text{ plus } 3 : \textsc{Int}$$

Recursive Typing Rules

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}} \; (t\text{-}plus)$$

$$\frac{v \in nat}{v : \textsc{Int}} \; (t\text{-}nat)$$

$$\Downarrow$$

$$\boxed{\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}} \; (t\text{-}plus)} \left[\begin{array}{lcl} e_1 & \mapsto & 1 \\ e_2 & \mapsto & 2 \text{ plus } 3 \end{array} \right]$$

$$1 \text{ plus } 2 \text{ plus } 3 : \textsc{Int}$$

Recursive Typing Rules

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}} \; (t\text{-}plus)$$

$$\frac{v \in nat}{v : \textsc{Int}} \; (t\text{-}nat)$$

$$\boxed{\frac{1 : \textsc{Int} \quad 2 \text{ plus } 3 : \textsc{Int}}{1 \text{ plus } 2 \text{ plus } 3 : \textsc{Int}} \; (t\text{-}plus)}$$

$1 \text{ plus } 2 \text{ plus } 3 : \textsc{Int}$

Recursive Typing Rules

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}} \; (\textit{t-plus})$$

$$\frac{v \in \textit{nat}}{v : \textsc{Int}} \; (\textit{t-nat})$$

$$\frac{1 : \textsc{Int} \qquad\qquad 2 \text{ plus } 3 : \textsc{Int}}{1 \text{ plus } 2 \text{ plus } 3 : \textsc{Int}} \; (\textit{t-plus})$$

Recursive Typing Rules

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}} \; (\textit{t-plus})$$

$$\frac{v \in \textit{nat}}{v : \textsc{Int}} \; (\textit{t-nat})$$

$$\Downarrow$$

$$\boxed{\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}} \; (\textit{t-plus})}$$

$$\frac{1 : \textsc{Int} \qquad\qquad 2 \text{ plus } 3 : \textsc{Int}}{1 \text{ plus } 2 \text{ plus } 3 : \textsc{Int}} \; (\textit{t-plus})$$

Recursive Typing Rules

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}} \; (\textit{t-plus})$$

$$\frac{v \in \textit{nat}}{v : \textsc{Int}} \; (\textit{t-nat})$$

$$\boxed{\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}} \; (\textit{t-plus})} \left[\begin{array}{lcl} e_1 & \mapsto & 2 \\ e_2 & \mapsto & 3 \end{array} \right]$$

$$\frac{1 : \textsc{Int} \qquad\qquad 2 \text{ plus } 3 : \textsc{Int}}{1 \text{ plus } 2 \text{ plus } 3 : \textsc{Int}} \; (\textit{t-plus})$$

Recursive Typing Rules

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}} \; (\textit{t-plus})$$

$$\frac{v \in \textit{nat}}{v : \textsc{Int}} \; (\textit{t-nat})$$

$$\boxed{\frac{2 : \textsc{Int} \quad 3 : \textsc{Int}}{2 \text{ plus } 3 : \textsc{Int}} \; (\textit{t-plus})}$$

$$\frac{1 : \textsc{Int} \qquad\qquad 2 \text{ plus } 3 : \textsc{Int}}{1 \text{ plus } 2 \text{ plus } 3 : \textsc{Int}} \; (\textit{t-plus})$$

Recursive Typing Rules

$$\frac{e_1 : \textsc{Int} \qquad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}} \; (\textit{t-plus})$$

$$\frac{v \in \textit{nat}}{v : \textsc{Int}} \; (\textit{t-nat})$$

$$\frac{1 : \textsc{Int} \qquad \dfrac{2 : \textsc{Int} \qquad 3 : \textsc{Int}}{2 \text{ plus } 3 : \textsc{Int}} \; (\textit{t-plus})}{1 \text{ plus } 2 \text{ plus } 3 : \textsc{Int}} \; (\textit{t-plus})$$

Recursive Typing Rules

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}} \; (t\text{-}plus)$$

$$\frac{v \in nat}{v : \textsc{Int}} \; (t\text{-}nat)$$

$$\frac{1 : \textsc{Int} \qquad \dfrac{2 : \textsc{Int} \qquad 3 : \textsc{Int}}{2 \text{ plus } 3 : \textsc{Int}} \; (t\text{-}plus)}{1 \text{ plus } 2 \text{ plus } 3 : \textsc{Int}} \; (t\text{-}plus)$$

Recursive Typing Rules

$$\frac{e_1 : \textsc{Int} \qquad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}}\ (\textit{t-plus})$$

$$\frac{v \in \textit{nat}}{v : \textsc{Int}}\ (\textit{t-nat})$$

$[v \mapsto 1]$

$[v \mapsto 2]$

$[v \mapsto 3]$

$$\frac{1 \in \textit{nat}}{1 : \textsc{Int}}\ (\textit{t-nat}) \qquad \frac{2 \in \textit{nat}}{2 : \textsc{Int}}\ (\textit{t-nat}) \qquad \frac{3 \in \textit{nat}}{3 : \textsc{Int}}\ (\textit{t-nat})$$

$$\frac{1 : \textsc{Int} \qquad \dfrac{2 : \textsc{Int} \qquad 3 : \textsc{Int}}{2 \text{ plus } 3 : \textsc{Int}}\ (\textit{t-plus})}{1 \text{ plus } 2 \text{ plus } 3 : \textsc{Int}}\ (\textit{t-plus})$$

Recursive Typing Rules

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}} \; (t\text{-}plus)$$

$$\frac{v \in nat}{v : \textsc{Int}} \; (t\text{-}nat)$$

$$\frac{\dfrac{1 \in nat}{1 : \textsc{Int}} \; (t\text{-}nat) \qquad \dfrac{\dfrac{2 \in nat}{2 : \textsc{Int}} \; (t\text{-}nat) \qquad \dfrac{3 \in nat}{3 : \textsc{Int}} \; (t\text{-}nat)}{2 \text{ plus } 3 : \textsc{Int}} \; (t\text{-}plus)}{1 \text{ plus } 2 \text{ plus } 3 : \textsc{Int}} \; (t\text{-}plus)$$

Recursive Typing Rules

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}} \; (t\text{-}plus)$$

$$\frac{v \in nat}{v : \textsc{Int}} \; (t\text{-}nat)$$

$$\frac{\dfrac{1 \in nat}{1 : \textsc{Int}} \; (t\text{-}nat) \qquad \dfrac{\dfrac{2 \in nat}{2 : \textsc{Int}} \; (t\text{-}nat) \quad \dfrac{3 \in nat}{3 : \textsc{Int}} \; (t\text{-}nat)}{2 \text{ plus } 3 : \textsc{Int}} \; (t\text{-}plus)}{1 \text{ plus } 2 \text{ plus } 3 : \cancel{\textsc{Int}}} \; (t\text{-}plus)$$

Types for Expressions

$$\frac{}{\mathsf{true} : \textsc{Bool}}\ (\textit{t-true}) \qquad \frac{}{\mathsf{false} : \textsc{Bool}}\ (\textit{t-false}) \qquad \frac{v \in \textit{nat}}{v : \textsc{Int}}\ (\textit{t-nat})$$

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1\ \mathsf{plus}\ e_2 : \textsc{Int}}\ (\textit{t-plus})$$

Types for Expressions

$$\frac{}{\text{true} : \textsc{Bool}}\ (t\text{-}true) \qquad \frac{}{\text{false} : \textsc{Bool}}\ (t\text{-}false) \qquad \frac{v \in nat}{v : \textsc{Int}}\ (t\text{-}nat)$$

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}}\ (t\text{-}plus) \qquad \frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 >= e_2 : \textsc{Bool}}\ (t\text{-}ge)$$

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \textsc{Int} \quad e_3 : \textsc{Int}}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \textsc{Int}}\ (t\text{-}if\text{-}nat)$$

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \textsc{Bool} \quad e_3 : \textsc{Bool}}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \textsc{Bool}}\ (t\text{-}if\text{-}bool)$$

Types for Expressions

$$\frac{}{\text{true} : \textsc{Bool}}\ (t\text{-}true) \qquad \frac{}{\text{false} : \textsc{Bool}}\ (t\text{-}false) \qquad \frac{v \in nat}{v : \textsc{Int}}\ (t\text{-}nat)$$

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}}\ (t\text{-}plus) \qquad \frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 >= e_2 : \textsc{Bool}}\ (t\text{-}ge)$$

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \tau \quad e_3 : \tau}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \tau}\ (t\text{-}if)$$

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \textsc{Int} \quad e_3 : \textsc{Int}}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \textsc{Int}}\ (t\text{-}if\text{-}nat)$$

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \textsc{Bool} \quad e_3 : \textsc{Bool}}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \textsc{Bool}}\ (t\text{-}if\text{-}bool)$$

(*if*) rule summarises (*if-nat*) and (*if-bool*) via *type variable*

Checking Types

- With $e : \tau$, we can have:

1. Exactly one τ fits (we've computed a type):

$$2 \text{ plus } 3 : \textsc{Int}$$

2. No τ fits (type error):

$$\textit{Type error in } \text{true plus } 0$$

3. Multiple τ fit: can't happen in this type system

Inferring Types

$x + y$

- Checking explores "*is everything consistent?*"
- Inferring explores "*what is possible?*"
- In program analysis, we often want the latter. Recall:

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \tau \quad e_3 : \tau}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \tau} \; (\textit{t-if})$$

- What if we don't care for consistency and instead simply want to know all options (e.g., for optimisation)?

Inferring Types

- Checking explores "*is everything consistent?*"
- Inferring explores "*what is possible?*"
- In program analysis, we often want the latter. Recall:

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \tau \quad e_3 : \tau}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \tau} \; (t\text{-}if)$$

syn Type Expr.type().

- What if we don't care for consistency and instead simply want to know all options (e.g., for optimisation)?
- The following rule may be a better fit:

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \tau_2 \quad e_3 : \tau_3 \quad i \in \{2, 3\}}{\underline{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3} : \tau_i} \; (t\text{-}if')$$

true 22 : Bool Int

Inferring Types

- Checking explores "*is everything consistent?*"
- Inferring explores "*what is possible?*"
- In program analysis, we often want the latter. Recall:

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \tau \quad e_3 : \tau}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \tau} \; (t\text{-}if)$$

- What if we don't care for consistency and instead simply want to know all options (e.g., for optimisation)?
- The following rule may be a better fit:

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \tau_2 \quad e_3 : \tau_3 \quad i \in \{2, 3\}}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \tau_i} \; (t\text{-}if')$$

- For efficiency, we then sometimes store types in sets ('Set Types') and use notation such as:

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \tau_2 \quad e_3 : \tau_3}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \underline{\tau_2 \cup \tau_3}} \; (t\text{-}if'')$$

- We can design type rules so that set types always produce

Summary

- *Type systems* relate expressions to types:

$$(:) \subseteq \mathit{expr} \times \mathbb{T}_{iga}$$

- We use *inference rules* to compactly describe the type system

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \tau \quad e_3 : \tau}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \tau} \; (t\text{-}if)$$

- No type matches $\Rightarrow$ type error
- We will focus on Type Checking for a bit, for simplicity

Adding Variables: The language INGA

$$
\begin{array}{lcll}
\mathit{expr} & ::= & \langle \mathit{val} \rangle & \\
 & | & \mathit{id} & \textbf{new!} \\
 & | & \text{let } \mathit{id} = \langle \mathit{expr} \rangle \text{ in } \langle \mathit{expr} \rangle & \textbf{new!} \\
 & | & \langle \mathit{expr} \rangle \text{ plus } \langle \mathit{expr} \rangle & \\
 & | & \langle \mathit{expr} \rangle >= \langle \mathit{expr} \rangle & \\
 & | & \text{if } \langle \mathit{expr} \rangle \text{ then } \langle \mathit{expr} \rangle \text{ else } \langle \mathit{expr} \rangle & \\
 & & & \\
\mathit{val} & ::= & \mathit{nat} & \\
 & | & \text{true} \mid \text{false} & \\
 & & & \\
\mathit{nat} & ::= & 0 \mid 1 \mid 2 \mid 3 \mid 4 \mid \ldots & \\
\mathit{id} & ::= & \underline{x} \mid \underline{y} \mid \underline{z} \mid \ldots &
\end{array}
$$

- Adds locally scoped variable bindings
- let $\underline{x}$ = 1 plus 2 in $\underline{x}$ + 3 evaluates to 6
- let $\underline{x}$ = 1 in (let $\underline{x}$ = 2 in $\underline{x}$) + $\underline{x}$ evaluates to 3

Typing Variables

$$\frac{}{\text{true} : \textsc{Bool}}\ (t\text{-}true) \qquad \frac{}{\text{false} : \textsc{Bool}}\ (t\text{-}false) \qquad \frac{v \in nat}{v : \textsc{Int}}\ (t\text{-}nat)$$

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}}\ (t\text{-}plus) \qquad \frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 >= e_2 : \textsc{Bool}}\ (t\text{-}ge) \qquad \frac{e_1 : \textsc{Bool} \quad e_2 : \tau \quad e_3 : \tau}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \tau}\ (t\text{-}if)$$

- Same types as before: $\mathbb{T}_{inga} = \{\textsc{Bool}, \textsc{Int}\}$
- Need new typing rules for let and variables:

$$\frac{e_2 : \tau_2}{\text{let } \underline{x} = e_1 \text{ in } e_2 : \tau_2}\ t\text{-}let$$

Typing Variables

$$\frac{}{\text{true} : \textsc{Bool}}\ (t\text{-}true) \qquad \frac{}{\text{false} : \textsc{Bool}}\ (t\text{-}false) \qquad \frac{v \in nat}{v : \textsc{Int}}\ (t\text{-}nat)$$

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}}\ (t\text{-}plus) \qquad \frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 >= e_2 : \textsc{Bool}}\ (t\text{-}ge) \qquad \frac{e_1 : \textsc{Bool} \quad e_2 : \tau \quad e_3 : \tau}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \tau}\ (t\text{-}if)$$

- Same types as before: $\mathbb{T}_{inga} = \{\textsc{Bool}, \textsc{Int}\}$
- Need new typing rules for let and variables:

$$\frac{e_1 : \tau_1 \quad e_2 : \tau_2}{\text{let } \underline{x} = e_1 \text{ in } e_2 : \tau_2}\ t\text{-}let$$

Typing Variables

$$\frac{}{\text{true} : \textsc{Bool}}\ (t\text{-}true) \qquad \frac{}{\text{false} : \textsc{Bool}}\ (t\text{-}false) \qquad \frac{v \in nat}{v : \textsc{Int}}\ (t\text{-}nat)$$

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}}\ (t\text{-}plus) \qquad \frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 >= e_2 : \textsc{Bool}}\ (t\text{-}ge) \qquad \frac{e_1 : \textsc{Bool} \quad e_2 : \tau \quad e_3 : \tau}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \tau}\ (t\text{-}if)$$

- Same types as before: $\mathbb{T}_{inga} = \{\textsc{Bool}, \textsc{Int}\}$
- Need new typing rules for let and variables:

$$\frac{}{\underline{x} : \tau}\ t\text{-}var$$

$$\frac{e_1 : \tau_1 \quad e_2 : \tau_2}{\text{let } \underline{x} = e_1 \text{ in } e_2 : \tau_2}\ t\text{-}let$$

How do we connect τ_1 and τ and τ_2 ?

Connecting Variables and Types

$$\frac{e_1 : \tau_1 \quad e_2 : \tau_2}{\text{let } \underline{x} = e_1 \text{ in } e_2 : \tau_2}\ \textit{t-let} \quad \xleftrightarrow{?} \quad \frac{}{\underline{x} : \tau}\ \textit{t-var}$$

- We know that $\underline{x} : \tau_1$ before we analyse e_2
- Must carry this information into the analysis of e_2:
- Can be solved with typing rules with a bit of extra notation:

$$\frac{\Gamma \vdash e_1 : \tau_1 \quad \Gamma[\underline{x} \mapsto \tau_1] \vdash e_2 : \tau_2}{\Gamma \vdash \text{let } \underline{x} = e_1 \text{ in } e_2 : \tau_2}\ \textit{t-let}$$

Connecting Variables and Types

$$\frac{e_1 : \tau_1 \quad e_2 : \tau_2}{\text{let } \underline{x} = e_1 \text{ in } e_2 : \tau_2}\ \textit{t-let} \quad \xleftrightarrow{?} \quad \frac{}{\underline{x} : \tau}\ \textit{t-var}$$

- We know that $\underline{x} : \tau_1$ before we analyse e_2
- Must carry this information into the analysis of e_2:
- Can be solved with typing rules with a bit of extra notation:

$$\frac{\Gamma \vdash e_1 : \tau_1 \quad \Gamma[\underline{x} \mapsto \tau_1] \vdash e_2 : \tau_2}{\Gamma \vdash \text{let } \underline{x} = e_1 \text{ in } e_2 : \tau_2}\ \textit{t-let}$$

This notation does't reflect how we would solve name/type analysis in Java / Scala / JastAdd.

Variables and Types in Practice

$$\frac{e_1 : \tau_1 \quad e_2 : \tau_2}{\text{let } \underline{x} = e_1 \text{ in } e_2 : \tau_2}\ \textit{t-let} \quad \xleftrightarrow{?} \quad \frac{}{\underline{x} : \tau}\ \textit{t-var}$$

- Instead, we will cheat:
  - Write $\boxed{\underline{x}\texttt{.ty} = \tau}$ to *assert* type of $\underline{x}$
  - Semantics:
    - If $\underline{x}$`.ty` unset, assign τ
    - Otherwise check equality
  - For now only works if we analyse top-down (more later, though!)
- **Note**: these attributes are associated with the *variable declarations* / *symbol table entries*:

$$\text{let } \underline{x} = 1 \text{ in let } \underline{x} = \text{true in } \underline{x} : \textsc{Bool}$$

- Equivalently, assume that all variables have unique names.

Typing INGA

$$\frac{}{\mathsf{true} : \textsc{Bool}}\ (\textit{t-true}) \qquad \frac{}{\mathsf{false} : \textsc{Bool}}\ (\textit{t-false}) \qquad \frac{v \in \textit{nat}}{v : \textsc{Int}}\ (\textit{t-nat})$$

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \ \mathsf{plus}\ e_2 : \textsc{Int}}\ (\textit{t-plus}) \qquad \frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 >= e_2 : \textsc{Bool}}\ (\textit{t-ge})$$

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \tau \quad e_3 : \tau}{\textbf{if}\ e_1\ \textbf{then}\ e_2\ \textbf{else}\ e_3 : \tau}\ (\textit{t-if})$$

$$\frac{e_1 : \tau_1 \quad \underline{x}.\mathtt{ty} = \tau_1 \quad e_2 : \tau_2}{\mathsf{let}\ \underline{x} = e_1\ \mathsf{in}\ e_2 : \tau_2}\ \textit{t-let} \qquad \frac{\underline{x}.\mathtt{ty} = \tau}{\underline{x} : \tau}\ \textit{t-var}$$

Example

$$\frac{}{\text{true} : \textsc{Bool}}\ (t\text{-}true) \qquad \frac{}{\text{false} : \textsc{Bool}}\ (t\text{-}false) \qquad \frac{v \in nat}{v : \textsc{Int}}\ (t\text{-}nat)$$

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}}\ (t\text{-}plus) \qquad \frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 >= e_2 : \textsc{Bool}}\ (t\text{-}ge) \qquad \frac{x.\texttt{ty} = \tau}{x : \tau}\ (t\text{-}var)$$

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \tau \quad e_3 : \tau}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \tau}\ (t\text{-}if) \qquad \frac{e_1 : \tau_1 \quad x.\texttt{ty} = \tau_1 \quad e_2 : \tau_2}{\text{let } x = e_1 \text{ in } e_2 : \tau_2}\ (t\text{-}let)$$

$$\boxed{x.ty = \textsc{Int}}$$

$$\frac{1 \in nat}{1 : \textsc{Int}}\ t\text{-}nat \qquad x.ty = \textsc{Int} \qquad \frac{\dfrac{x.ty = \textsc{Int}}{x : \textsc{Int}}\ t\text{-}var \qquad x : \textsc{Int}}{x \text{ plus } x : \tau_2}\ t\text{-}plus$$

$$\frac{}{\text{let } x = 1 \text{ in } x \text{ plus } x : \tau_2}\ (t\text{-}let)$$

Example

$$\frac{}{\text{true} : \textsc{Bool}}\ (\textit{t-true}) \qquad \frac{}{\text{false} : \textsc{Bool}}\ (\textit{t-false}) \qquad \frac{v \in \textit{nat}}{v : \textsc{Int}}\ (\textit{t-nat})$$

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}}\ (\textit{t-plus}) \qquad \frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 >= e_2 : \textsc{Bool}}\ (\textit{t-ge}) \qquad \frac{\underline{x}.\texttt{ty} = \tau}{\underline{x} : \tau}\ (\textit{t-var})$$

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \tau \quad e_3 : \tau}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \tau}\ (\textit{t-if}) \qquad \frac{e_1 : \tau_1 \quad \underline{x}.\texttt{ty} = \tau_1 \quad e_2 : \tau_2}{\text{let } \underline{x} = e_1 \text{ in } e_2 : \tau_2}\ (\textit{t-let})$$

$$\boxed{\underline{x}.\texttt{ty} = \textsc{Int}}$$

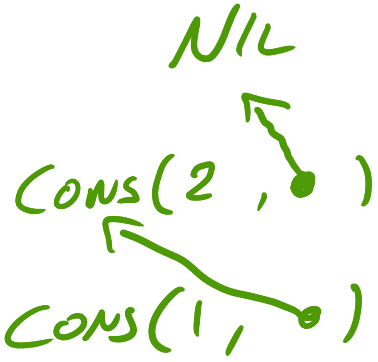
$$\frac{\dfrac{1 \in \textit{nat}}{1 : \textsc{Int}}\ (\textit{t-nat}) \qquad \underline{x}.\texttt{ty} = \textsc{Int} \qquad \dfrac{\dfrac{\underline{x}.\texttt{ty} = \textsc{Int}}{\underline{x} : \textsc{Int}}\ (\textit{t-var}) \quad \dfrac{\underline{x}.\texttt{ty} = \textsc{Int}}{\underline{x} : \textsc{Int}}\ (\textit{t-var})}{\underline{x} \text{ plus } \underline{x} : \textsc{Int}}\ (\textit{t-plus})}{\text{let } \underline{x} = 1 \text{ in } \underline{x} \text{ plus } \underline{x} : \textsc{Int}}\ (\textit{t-let})$$

Summary

- To analyse realistic programs, we must analyse name bindings
- We do so through *indirection*:
  - Assume that we associate names with declarations / symbol table entries
  - When we encounter a name and want to:
    - *type-check*: if type not bound, set it now, otherwise check
    - *read type*: only works if type is already bound

Adding Lists: The Language LINGA

$$
\begin{array}{lcll}
\mathit{expr} & ::= & \langle \mathit{val} \rangle & \\
 & | & \mathit{id} & \\
 & | & \text{let } \mathit{id} = \langle \mathit{expr} \rangle \text{ in } \langle \mathit{expr} \rangle & \\
 & | & \text{nil} \quad \text{value} \quad \text{list} & \textbf{new!} \\
 & | & \text{cons } (\langle \mathit{expr} \rangle, \langle \mathit{expr} \rangle) & \textbf{new!} \\
 & | & \langle \mathit{expr} \rangle \text{ plus } \langle \mathit{expr} \rangle & \\
 & | & \langle \mathit{expr} \rangle >= \langle \mathit{expr} \rangle & \\
 & | & \text{if } \langle \mathit{expr} \rangle \text{ then } \langle \mathit{expr} \rangle \text{ else } \langle \mathit{expr} \rangle & \\
 & & & \\
\mathit{val} & ::= & \mathit{nat} & \\
 & | & \text{true} \ | \ \text{false} &
\end{array}
$$



- nil is the empty list
- cons(v, ℓ) takes list ℓ and prepends v
- Can express list [0, 1, 2] as:

$$\text{cons}(0, \text{cons}(1, \text{cons}(2, \text{nil})))$$

The Type of Lists

The language of types $\mathbb{T}_{linga}$ has one new production:

$$
\begin{array}{rcl}
ty & ::= & \textsc{Int} \\
 & | & \textsc{Bool} \\
 & | & \textsc{List}\ [\langle ty \rangle]
\end{array}
$$

The Type of Lists

The language of types $\mathbb{T}_{linga}$ has one new production:

$$
\begin{array}{rcl}
ty & ::= & \textsc{Int} \\
 & | & \textsc{Bool} \\
 & | & \textsc{List}\ [\langle ty \rangle]
\end{array}
$$

Example types:

- cons(true, nil) : $\textsc{List}[\textsc{Bool}]$
- cons(1, cons(2, nil)) : $\textsc{List}[\textsc{Int}]$
- cons(1, cons(false, nil)) :

The Type of Lists

The language of types $\mathbb{T}_{linga}$ has one new production:

$$
\begin{array}{rcl}
ty & ::= & \textsc{Int} \\
 & | & \textsc{Bool} \\
 & | & \textsc{List}\ [\langle ty \rangle]
\end{array}
$$

Example types:

- cons(true, nil) : $\textsc{List}[\textsc{Bool}]$
- cons(1, cons(2, nil)) : $\textsc{List}[\textsc{Int}]$
- cons(1, cons(false, nil)) : ?

First attempt at typing rules:

$$\frac{\tau \in \mathbb{T}_{linga}}{\text{nil} : \textsc{List}[\tau]}\ (t\text{-}nil)$$

$$\frac{e_1 : \tau \quad e_2 : \textsc{List}[\tau]}{\text{cons}(e_1, e_2) : \textsc{List}[\tau]}\ (t\text{-}cons)$$

The Type of Lists

The language of types $\mathbb{T}_{linga}$ has one new production:

$$
\begin{array}{rcl}
ty & ::= & \textsc{Int} \\
 & | & \textsc{Bool} \\
 & | & \textsc{List}\ [\langle ty \rangle]
\end{array}
$$

Example types:

- cons(true, nil) : $\textsc{List}[\textsc{Bool}]$
- cons(1, cons(2, nil)) : $\textsc{List}[\textsc{Int}]$
- cons(1, cons(false, nil)) : *type error*

First attempt at typing rules:

$$\frac{\tau \in \mathbb{T}_{linga}}{\text{nil} : \textsc{List}[\tau]}\ (t\text{-}nil)$$

$$\frac{e_1 : \tau \quad e_2 : \textsc{List}[\tau]}{\text{cons}(e_1,\ e_2) : \textsc{List}[\tau]}\ (t\text{-}cons)$$

The Type of Lists

The language of types $\mathbb{T}_{linga}$ has one new production:

$$
\begin{array}{rcl}
ty & ::= & \textsc{Int} \\
 & | & \textsc{Bool} \\
 & | & \textsc{List}\ [\langle ty \rangle]
\end{array}
$$

Example types:

- cons(true, nil) : $\textsc{List}[\textsc{Bool}]$
- cons(1, cons(2, nil)) : $\textsc{List}[\textsc{Int}]$
- cons(1, cons(false, nil)) : *type error*
- cons(cons(1, nil), nil) : $\textsc{List}[\textsc{List}[\textsc{Int}]]$
- nil : List [INT]

First attempt at typing rules:

$$\frac{\tau \in \mathbb{T}_{linga}}{\text{nil} : \textsc{List}[\tau]}\ (t\text{-}nil)$$

$$\frac{e_1 : \tau \quad e_2 : \textsc{List}[\tau]}{\text{cons}(e_1,\ e_2) : \textsc{List}[\tau]}\ (t\text{-}cons)$$

x : ?

let x = nil in ..... nil .. x ...

The Type of Lists

The language of types $\mathbb{T}_{linga}$ has one new production:

$$
\begin{array}{rcl}
ty & ::= & \textsc{Int} \\
 & | & \textsc{Bool} \\
 & | & \textsc{List}\ [\langle ty \rangle]
\end{array}
$$

Example types:

- cons(true, nil) : $\textsc{List}[\textsc{Bool}]$
- cons(1, cons(2, nil)) : $\textsc{List}[\textsc{Int}]$
- cons(1, cons(false, nil)) : *type error*
- cons(cons(1, nil), nil) : $\textsc{List}[\textsc{List}[\textsc{Int}]]$
- nil : $\textsc{List}[\textsc{Int}]$
  $\textsc{List}[\textsc{Bool}]$
  $\textsc{List}[\textsc{List}[\textsc{Int}]]$
  $\textsc{List}[\ldots, \textsc{List}[\textsc{Bool}], \ldots]$

First attempt at typing rules:

$$\frac{\tau \in \mathbb{T}_{linga}}{\text{nil} : \textsc{List}[\tau]}\ (t\text{-}nil)$$

$$\frac{e_1 : \tau \quad e_2 : \textsc{List}[\tau]}{\text{cons}(e_1, e_2) : \textsc{List}[\tau]}\ (t\text{-}cons)$$

The Type of Lists

The language of types $\mathbb{T}_{linga}$ has one new production:

$$
\begin{array}{rcl}
ty & ::= & \textsc{Int} \\
 & | & \textsc{Bool} \\
 & | & \textsc{List}\ [\langle ty \rangle]
\end{array}
$$

Example types:

- cons(true, nil) : $\textsc{List}[\textsc{Bool}]$
- cons(1, cons(2, nil)) : $\textsc{List}[\textsc{Int}]$
- cons(1, cons(false, nil)) : *type error*
- cons(cons(1, nil), nil) : $\textsc{List}[\textsc{List}[\textsc{Int}]]$
- nil : $\textsc{List}[\textsc{Int}]$
  $\textsc{List}[\textsc{Bool}]$
  $\textsc{List}[\textsc{List}[\textsc{Int}]]$
  $\textsc{List}[\ldots, \textsc{List}[\textsc{Bool}], \ldots]$

First attempt at typing rules:

$$\frac{\tau \in \mathbb{T}_{linga}}{\text{nil} : \textsc{List}[\tau]}\ (t\text{-}nil)$$

$$\frac{e_1 : \tau \quad e_2 : \textsc{List}[\tau]}{\text{cons}(e_1, e_2) : \textsc{List}[\tau]}\ (t\text{-}cons)$$

nil has infinitely many of the types in $\mathbb{T}_{linga}$

Type Variables

$$
\begin{array}{lcl}
ty & ::= & \textsc{Int} \\
 & | & \textsc{Bool} \\
 & | & \textsc{List}\ [\langle ty \rangle]
\end{array}
$$

- Working with infinitely many types is impractical

Type Variables

$$
\begin{array}{lcl}
\mathit{ty} & ::= & \textsc{Int} \\
 & | & \textsc{Bool} \\
 & | & \textsc{List}\ [\langle \mathit{ty} \rangle] \\
 & | & \mathit{tyvar} \\
\mathit{tyvar} & ::= & \alpha \mid \beta \mid \gamma \mid \ldots
\end{array}
$$

- Working with infinitely many types is impractical
- Summarise types by introducing *type variables* into $\mathbb{T}_{\mathit{linga}}$
- Can now define type of nil:

$$\frac{}{\mathsf{nil} : \textsc{List}[\alpha]}\ (\textit{t-nil})$$

Type Variables

$$
\begin{array}{lcl}
\mathit{ty} & ::= & \textsc{Int} \\
 & | & \textsc{Bool} \\
 & | & \textsc{List}\ [\langle \mathit{ty} \rangle] \\
 & | & \mathit{tyvar} \\
 & & \\
\mathit{tyvar} & ::= & \alpha \mid \beta \mid \gamma \mid \ldots
\end{array}
$$

- Working with infinitely many types is impractical
- Summarise types by introducing *type variables* into $\mathbb{T}_{\mathit{linga}}$
- Can now define type of nil:

$$\frac{}{\mathsf{nil} : \textsc{List}[\alpha]}\ (\mathit{t\text{-}nil})$$

We call types that can summarise all possible types in this fashion principal types

Three Languages With Variables

Meta-Language

- Describes *Object Language*(s)
- Variables refer to object language concepts:
  - LINGA programs
  - $\mathbb{T}_{linga}$ types

Programs: LINGA

- "Object Language" #1
- Variables refer to input programs
- Example: $\underline{x}$ in

$$\text{let } \underline{x} = 1 \text{ in } \underline{x}$$

Types: $\mathbb{T}_{linga}$

- "Object Language" #2
- Variables refer to unknown types
- Example: α in

$$\textsc{List}[\alpha]$$

Meta-Variables Can Reference Object-Language Variables

Meta-Variable references	Example	Meta-Variable Notation
Program	1 plus 2	e
Type	$\textsc{List}[\textsc{Bool}]$	τ
Program variable	$\underline{\text{foo}}$	$\underline{x}$
Type Variable	α	α

Typing Rules for Parametric Types

$$\frac{}{\mathsf{true} : \textsc{Bool}}\ (\textit{t-true}) \qquad \frac{}{\mathsf{false} : \textsc{Bool}}\ (\textit{t-false}) \qquad \frac{v \in \textit{nat}}{v : \textsc{Int}}\ (\textit{t-nat})$$

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1\ \mathsf{plus}\ e_2 : \textsc{Int}}\ (\textit{t-plus}) \qquad \frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 >= e_2 : \textsc{Bool}}\ (\textit{t-ge}) \qquad \frac{\underline{x}.\mathtt{ty} = \tau}{\underline{x} : \tau}\ (\textit{t-var})$$

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \tau \quad e_3 : \tau}{\textbf{if}\ e_1\ \textbf{then}\ e_2\ \textbf{else}\ e_3 : \tau}\ (\textit{t-if}) \qquad \frac{e_1 : \tau_1 \quad \underline{x}.\mathtt{ty} = \tau_1 \quad e_2 : \tau_2}{\mathsf{let}\ \underline{x} = e_1\ \mathsf{in}\ e_2 : \tau_2}\ (\textit{t-let})$$

$$\frac{}{\mathsf{nil} : \textsc{List}[\alpha]}\ (\textit{t-nil}) \qquad \frac{e_1 : \tau \quad e_2 : \textsc{List}[\tau]}{\mathsf{cons}(e_1, e_2) : \textsc{List}[\tau]}\ (\textit{t-cons})$$

Typing Rules for Parametric Types

$$\frac{}{\text{true} : \textsc{Bool}}\ (t\text{-}true) \qquad \frac{}{\text{false} : \textsc{Bool}}\ (t\text{-}false) \qquad \frac{v \in nat}{v : \textsc{Int}}\ (t\text{-}nat)$$

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}}\ (t\text{-}plus) \qquad \frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 >= e_2 : \textsc{Bool}}\ (t\text{-}ge) \qquad \frac{\underline{x}.\texttt{ty} = \tau}{\underline{x} : \tau}\ (t\text{-}var)$$

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \tau \quad e_3 : \tau}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \tau}\ (t\text{-}if) \qquad \frac{e_1 : \tau_1 \quad \underline{x}.\texttt{ty} = \tau_1 \quad e_2 : \tau_2}{\text{let } \underline{x} = e_1 \text{ in } e_2 : \tau_2}\ (t\text{-}let)$$

$$\frac{}{\text{nil} : \textsc{List}[\alpha]}\ (t\text{-}nil) \qquad \frac{e_1 : \tau \quad e_2 : \textsc{List}[\tau]}{\text{cons}(e_1, e_2) : \textsc{List}[\tau]}\ (t\text{-}cons)$$

$x.ty = List[\alpha] = List[INT]$

$List[\alpha] = List[INT]$

$\alpha.ty = INT$

$$\frac{\dfrac{}{nil : List[\alpha]}\ t\text{-}nil \qquad x.ty = List[\alpha] \qquad \dfrac{1 : INT \quad \dfrac{}{x : List[INT]}\ t\text{-}var}{cons(1, x) : List[\ ]}\ t\text{-}cons}{\text{let } \underline{x} = \text{nil in cons}(1, \underline{x}) : \textsc{List}[\textsc{Int}]}\ (t\text{-}let)$$

Typing Rules for Parametric Types

$$\frac{}{\text{true} : \textsc{Bool}}\ (t\text{-}true) \qquad \frac{}{\text{false} : \textsc{Bool}}\ (t\text{-}false) \qquad \frac{v \in nat}{v : \textsc{Int}}\ (t\text{-}nat)$$

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}}\ (t\text{-}plus) \qquad \frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 >= e_2 : \textsc{Bool}}\ (t\text{-}ge) \qquad \frac{\underline{x}.\texttt{ty} = \tau}{\underline{x} : \tau}\ (t\text{-}var)$$

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \tau \quad e_3 : \tau}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \tau}\ (t\text{-}if) \qquad \frac{e_1 : \tau_1 \quad \underline{x}.\texttt{ty} = \tau_1 \quad e_2 : \tau_2}{\text{let } \underline{x} = e_1 \text{ in } e_2 : \tau_2}\ (t\text{-}let)$$

$$\frac{}{\text{nil} : \textsc{List}[\alpha]}\ (t\text{-}nil) \qquad \frac{e_1 : \tau \quad e_2 : \textsc{List}[\tau]}{\text{cons}\ldots}\ (t\text{-}cons)$$

Originally $\underline{x}.\texttt{ty} = \textsc{List}[\alpha]$

Must merge $\textsc{List}[\alpha] = \textsc{List}[\textsc{Int}]$

Analogous to variable types

$\underline{x}.\texttt{ty} = \cancel{\textsc{List}[\alpha]}\ \textsc{List}[\textsc{Int}]$

$\boxed{\alpha.\texttt{ty} = \textsc{Int}}$

$$\frac{\frac{}{\text{nil} : \textsc{List}[\alpha]}\ (t\text{-}nil) \qquad \underline{x}.\texttt{ty} = \textsc{List}[\alpha] \qquad \frac{\frac{1 \in nat}{1 : \textsc{Int}}\ (t\text{-}nat) \qquad \frac{\underline{x}.\texttt{ty} = \textsc{List}[\textsc{Int}]}{\underline{x} : \textsc{List}[\textsc{Int}]}}{\text{cons}(1, \underline{x}) : \textsc{List}[\textsc{Int}]}}{\text{let } \underline{x} = \text{nil in cons}(1, \underline{x}) : \textsc{List}[\textsc{Int}]}\ (t\text{-}let)$$

Typing Rules for Parametric Types

$$\frac{}{\text{true} : \textsc{Bool}}\ (t\text{-}true) \qquad \frac{}{\text{false} : \textsc{Bool}}\ (t\text{-}false) \qquad \frac{v \in nat}{v : \textsc{Int}}\ (t\text{-}nat)$$

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}}\ (t\text{-}plus) \qquad \frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 >= e_2 : \textsc{Bool}}\ (t\text{-}ge) \qquad \frac{\underline{x}.\texttt{ty} = \tau}{\underline{x} : \tau}\ (t\text{-}var)$$

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \tau \quad e_3 : \tau}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \tau}\ (t\text{-}if) \qquad \frac{e_1 : \tau_1 \quad \underline{x}.\texttt{ty} = \tau_1 \quad e_2 : \tau_2}{\text{let } \underline{x} = e_1 \text{ in } e_2 : \tau_2}\ (t\text{-}let)$$

$$\frac{}{\text{nil} : \textsc{List}[\alpha]}\ (t\text{-}nil) \qquad \frac{e_1 : \tau \quad e_2 : \textsc{List}[\tau]}{\text{cons}(e_1, e_2) : \textsc{List}[\tau]}\ (t\text{-}cons)$$

$\tau = \textsc{List}[\alpha]$

$\textsc{List}[\alpha] = \textsc{List}[\tau]$

$$\frac{\dfrac{}{\text{nil} : \tau}\ t\text{-}nil \qquad \dfrac{}{\text{nil} : \textsc{List}[\tau]}\ t\text{-}nil}{\text{cons}(\text{nil}, \text{nil}) :}\ (t\text{-}cons)$$

Typing Rules for Parametric Types

$$\frac{}{\text{true} : \textsc{Bool}}\ (t\text{-}true) \qquad \frac{}{\text{false} : \textsc{Bool}}\ (t\text{-}false) \qquad \frac{v \in nat}{v : \textsc{Int}}\ (t\text{-}nat)$$

$$\frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 \text{ plus } e_2 : \textsc{Int}}\ (t\text{-}plus) \qquad \frac{e_1 : \textsc{Int} \quad e_2 : \textsc{Int}}{e_1 >= e_2 : \textsc{Bool}}\ (t\text{-}ge) \qquad \frac{\underline{x}.\texttt{ty} = \tau}{\underline{x} : \tau}\ (t\text{-}var)$$

$$\frac{e_1 : \textsc{Bool} \quad e_2 : \tau \quad e_3 : \tau}{\textbf{if } e_1 \textbf{ then } e_2 \textbf{ else } e_3 : \tau}\ (t\text{-}if) \qquad \frac{e_1 : \tau_1 \quad \underline{x}.\texttt{ty} = \tau_1 \quad e_2 : \tau_2}{\text{let } \underline{x} = e_1 \text{ in } e_2 : \tau_2}\ (t\text{-}let)$$

$$\frac{}{\text{nil} : \textsc{List}[\alpha]}\ (t\text{-}nil) \qquad \frac{e_1 : \tau \quad e_2 : \textsc{List}[\tau]}{\text{cons}(e_1, e_2) : \textsc{List}[\tau]}\ (t\text{-}cons)$$

Circular type — *t-cons* requires:

$$\begin{aligned} \tau &= \textsc{List}[\alpha] \\ \textsc{List}[\tau] &= \textsc{List}[\alpha] \end{aligned}$$

$$\boxed{\alpha.\texttt{ty} = \textsc{List}[\alpha]}$$

$$\frac{\dfrac{}{\text{nil} : \textsc{List}[\alpha]}\ (t\text{-}nil) \qquad \dfrac{}{\text{nil} : \textsc{List}[\alpha]}\ (t\text{-}nil)}{\text{cons}(\text{nil}, \text{nil}) : \ ?}\ (t\text{-}cons)$$

Type Variable Freshness

- Our typing rule for nil doesn't work as intended:
  All nil use the same α in their type
  $\Longrightarrow$ all lists must have the same type

$$\frac{}{\mathsf{nil} : \textsc{List}[\alpha]}\ (\textit{t-nil}) \qquad \frac{e_1 : \tau \quad e_2 : \textsc{List}[\tau]}{\mathsf{cons}(e_1,\ e_2) : \textsc{List}[\tau]}\ (\textit{t-cons})$$

Type Variable Freshness

- Our typing rule for nil doesn't work as intended:
  All nil use the same α in their type
  $\Longrightarrow$ all lists must have the same type

$$\frac{\alpha \quad \textit{fresh}}{\mathsf{nil} : \textsc{List}[\alpha]}\ (\textit{t-nil}) \qquad \frac{e_1 : \tau \quad e_2 : \textsc{List}[\tau]}{\mathsf{cons}(e_1,\ e_2) : \textsc{List}[\tau]}\ (\textit{t-cons})$$

- Fix: We create a *fresh* type variable for every nil

$$\frac{}{\mathsf{cons}(\mathsf{nil},\ \mathsf{nil}) :}$$