CIS 500

Software Foundations

Fall 2002

21 October

Administrivia

- Missing HW5s have been found
- Notes on exam
  - Graded exams and answer key available from Christine (in 556)
  - Rough grade breakdown:
    - 65-80 points: A (32%)
    - 50-64 points: B (35%)
    - 35-49 points: C (19%)
    - $\leq$34 points: D/F (14%)

    60+ points is on-target for WPE-I
  - This exam mostly focused on the more “mechanical” aspects of the material we have seen. Future exams will be more focused on concepts (i.e., there will be more questions like 8, 9, 10, and 12).
- Grading questions? See your TA.

Sums - example

```
PhysicalAddr = {firstlast:String, addr:String}
VirtualAddr  = {name:String, email:String}
Addr         = PhysicalAddr + VirtualAddr
```

inl : "PhysicalAddr $\longrightarrow$ PhysicalAddr+VirtualAddr"

inr : "VirtualAddr $\longrightarrow$ PhysicalAddr+VirtualAddr"

```
getName = λa:Addr.
  case a of
    inl x ⇒ x.firstlast
  | inr y ⇒ y.name;
```

New syntactic forms

t	::=	...	terms
		inl t	tagging (left)
		inr t	tagging (right)
		case t of inl x⇒t | inr x⇒t	case
v	::=	...	values
		inl v	tagged value (left)
		inr v	tagged value (right)
T	::=	...	types
		T+T	sum type

New typing rules

$\boxed{\Gamma \vdash \texttt{t} : \texttt{T}}$

$$\frac{\Gamma \vdash \texttt{t}_1 : \texttt{T}_1}{\Gamma \vdash \texttt{inl}\ \texttt{t}_1 : \texttt{T}_1\texttt{+}\texttt{T}_2} \quad \text{(T-Inl)}$$

$$\frac{\Gamma \vdash \texttt{t}_1 : \texttt{T}_2}{\Gamma \vdash \texttt{inr}\ \texttt{t}_1 : \texttt{T}_1\texttt{+}\texttt{T}_2} \quad \text{(T-Inr)}$$

$$\frac{\begin{array}{c}\Gamma \vdash \texttt{t}_0 : \texttt{T}_1\texttt{+}\texttt{T}_2 \\ \Gamma, \texttt{x}_1\texttt{:}\texttt{T}_1 \vdash \texttt{t}_1 : \texttt{T} \qquad \Gamma, \texttt{x}_2\texttt{:}\texttt{T}_2 \vdash \texttt{t}_2 : \texttt{T}\end{array}}{\Gamma \vdash \texttt{case}\ \texttt{t}_0\ \texttt{of}\ \texttt{inl}\ \texttt{x}_1 \Rightarrow \texttt{t}_1\ \texttt{|}\ \texttt{inr}\ \texttt{x}_2 \Rightarrow \texttt{t}_2 : \texttt{T}} \quad \text{(T-Case)}$$

New evaluation rules

$\boxed{\mathtt{t} \longrightarrow \mathtt{t}'}$

$$\begin{array}{l}\mathtt{case\ (inl\ v_0\ )} \\ \mathtt{of\ inl\ x_1{\Rightarrow}t_1\ \mid\ inr\ x_2{\Rightarrow}t_2} \\ \qquad \longrightarrow [\mathtt{x_1} \mapsto \mathtt{v_0}]\mathtt{t_1}\end{array} \qquad \text{(E-CaseInl)}$$

$$\begin{array}{l}\mathtt{case\ (inr\ v_0\ )} \\ \mathtt{of\ inl\ x_1{\Rightarrow}t_1\ \mid\ inr\ x_2{\Rightarrow}t_2} \\ \qquad \longrightarrow [\mathtt{x_2} \mapsto \mathtt{v_0}]\mathtt{t_2}\end{array} \qquad \text{(E-CaseInr)}$$

$$\frac{\mathtt{t_0} \longrightarrow \mathtt{t_0'}}{\begin{array}{c}\mathtt{case\ t_0\ of\ inl\ x_1{\Rightarrow}t_1\ \mid\ inr\ x_2{\Rightarrow}t_2} \\ \longrightarrow \mathtt{case\ t_0'\ of\ inl\ x_1{\Rightarrow}t_1\ \mid\ inr\ x_2{\Rightarrow}t_2}\end{array}} \qquad \text{(E-Case)}$$

$$\frac{\texttt{t}_1 \longrightarrow \texttt{t}_1'}{\texttt{inl}\ \texttt{t}_1 \longrightarrow \texttt{inl}\ \texttt{t}_1'} \qquad \text{(E-InL)}$$

$$\frac{\texttt{t}_1 \longrightarrow \texttt{t}_1'}{\texttt{inr}\ \texttt{t}_1 \longrightarrow \texttt{inr}\ \texttt{t}_1'} \qquad \text{(E-InR)}$$

Sums and Uniqueness of Types

Problem:

If `t` has type `T`, then `inl t` has type `T+U` for every `U`.

I.e., we've lost uniqueness of types.

Possible solutions:

- "Infer" `U` as needed during typechecking
- Give constructors different names and only allow each name to appear in one sum type (requires generalization to "variants," which we'll see next) — OCaml's solution
- Annotate each `inl` and `inr` with the intended sum type.

For simplicity, let's choose the third.

New syntactic forms

`t`	::=	...	terms
		`inl t as T`	tagging (left)
		`inr t as T`	tagging (right)
`v`	::=	...	values
		`inl v as T`	tagged value (left)
		`inr v as T`	tagged value (right)

New typing rules

$\boxed{\Gamma \vdash \mathtt{t} : \mathtt{T}}$

$$\frac{\Gamma \vdash \mathtt{t}_1 : \mathtt{T}_1}{\Gamma \vdash \mathtt{inl}\ \mathtt{t}_1\ \mathtt{as}\ \mathtt{T}_1\mathtt{+}\mathtt{T}_2 : \mathtt{T}_1\mathtt{+}\mathtt{T}_2} \qquad \text{(T-INL)}$$

$$\frac{\Gamma \vdash \mathtt{t}_1 : \mathtt{T}_2}{\Gamma \vdash \mathtt{inr}\ \mathtt{t}_1\ \mathtt{as}\ \mathtt{T}_1\mathtt{+}\mathtt{T}_2 : \mathtt{T}_1\mathtt{+}\mathtt{T}_2} \qquad \text{(T-INR)}$$

Evaluation rules ignore annotations:

$$\boxed{\mathtt{t} \longrightarrow \mathtt{t}'}$$

$$\begin{array}{l} \mathtt{case}\ (\mathtt{inl}\ \mathtt{v}_0\ \mathtt{as}\ \mathtt{T}_0) \\ \mathtt{of}\ \mathtt{inl}\ \mathtt{x}_1 \Rightarrow \mathtt{t}_1 \mid \mathtt{inr}\ \mathtt{x}_2 \Rightarrow \mathtt{t}_2 \\ \qquad \longrightarrow [\mathtt{x}_1 \mapsto \mathtt{v}_0]\mathtt{t}_1 \end{array} \tag{E-CaseInl}$$

$$\begin{array}{l} \mathtt{case}\ (\mathtt{inr}\ \mathtt{v}_0\ \mathtt{as}\ \mathtt{T}_0) \\ \mathtt{of}\ \mathtt{inl}\ \mathtt{x}_1 \Rightarrow \mathtt{t}_1 \mid \mathtt{inr}\ \mathtt{x}_2 \Rightarrow \mathtt{t}_2 \\ \qquad \longrightarrow [\mathtt{x}_2 \mapsto \mathtt{v}_0]\mathtt{t}_2 \end{array} \tag{E-CaseInr}$$

$$\frac{\mathtt{t}_1 \longrightarrow \mathtt{t}_1'}{\mathtt{inl}\ \mathtt{t}_1\ \mathtt{as}\ \mathtt{T}_2 \longrightarrow \mathtt{inl}\ \mathtt{t}_1'\ \mathtt{as}\ \mathtt{T}_2} \tag{E-Inl}$$

$$\frac{\mathtt{t}_1 \longrightarrow \mathtt{t}_1'}{\mathtt{inr}\ \mathtt{t}_1\ \mathtt{as}\ \mathtt{T}_2 \longrightarrow \mathtt{inr}\ \mathtt{t}_1'\ \mathtt{as}\ \mathtt{T}_2} \tag{E-Inr}$$

Variants

Just as we generalized binary products to labeled records, we can generalize binary sums to labeled variants.

New syntactic forms

t	::=	...	terms
		`<l=t> as T`	tagging
		$\texttt{case t of <l}_i\texttt{=x}_i\texttt{>}\Rightarrow\texttt{t}_i\ ^{i\in 1..n}$	case
T	::=	...	types
		$\texttt{<l}_i\texttt{:T}_i\ ^{i\in 1..n}\texttt{>}$	type of variants

New evaluation rules

$\boxed{\mathtt{t} \longrightarrow \mathtt{t}'}$

$$\texttt{case (<}\mathtt{l}_j\texttt{=}\mathtt{v}_j\texttt{> as T) of <}\mathtt{l}_i\texttt{=}\mathtt{x}_i\texttt{>}\Rightarrow\mathtt{t}_i\ ^{i\in 1..n} \longrightarrow [\mathtt{x}_j \mapsto \mathtt{v}_j]\mathtt{t}_j \qquad \text{(E-CaseVariant)}$$

$$\frac{\mathtt{t}_0 \longrightarrow \mathtt{t}_0'}{\texttt{case }\mathtt{t}_0\texttt{ of <}\mathtt{l}_i\texttt{=}\mathtt{x}_i\texttt{>}\Rightarrow\mathtt{t}_i\ ^{i\in 1..n} \longrightarrow \texttt{case }\mathtt{t}_0'\texttt{ of <}\mathtt{l}_i\texttt{=}\mathtt{x}_i\texttt{>}\Rightarrow\mathtt{t}_i\ ^{i\in 1..n}} \qquad \text{(E-Case)}$$

$$\frac{\mathtt{t}_i \longrightarrow \mathtt{t}_i'}{\texttt{<}\mathtt{l}_i\texttt{=}\mathtt{t}_i\texttt{> as T} \longrightarrow \texttt{<}\mathtt{l}_i\texttt{=}\mathtt{t}_i'\texttt{> as T}} \qquad \text{(E-Variant)}$$

New typing rules

$$\boxed{\Gamma \vdash \mathtt{t} : \mathtt{T}}$$

$$\frac{\Gamma \vdash \mathtt{t}_j : \mathtt{T}_j}{\Gamma \vdash \mathtt{<l}_j\mathtt{=t}_j\mathtt{>}\ \mathtt{as}\ \mathtt{<l}_i\mathtt{:T}_i\ {}^{i\in 1..n}\mathtt{>} : \mathtt{<l}_i\mathtt{:T}_i\ {}^{i\in 1..n}\mathtt{>}} \qquad \text{(T-Variant)}$$

$$\frac{\Gamma \vdash \mathtt{t}_0 : \mathtt{<l}_i\mathtt{:T}_i\ {}^{i\in 1..n}\mathtt{>} \qquad \text{for each } i \quad \Gamma, \mathtt{x}_i\mathtt{:T}_i \vdash \mathtt{t}_i : \mathtt{T}}{\Gamma \vdash \mathtt{case}\ \mathtt{t}_0\ \mathtt{of}\ \mathtt{<l}_i\mathtt{=x}_i\mathtt{>}\Rightarrow\mathtt{t}_i\ {}^{i\in 1..n} : \mathtt{T}} \qquad \text{(T-Case)}$$

Examples

```
Addr = <physical:PhysicalAddr, virtual:VirtualAddr>;

a = <physical=pa> as Addr;

getName = λa:Addr.
  case a of
    <physical=x> ⇒ x.firstlast
  | <virtual=y> ⇒ y.name;
```

Options

Just like in OCaml...

```
OptionalNat = <none:Unit, some:Nat>;

Table = Nat→OptionalNat;

emptyTable = λn:Nat. <none=unit> as OptionalNat;

extendTable =
  λt:Table. λm:Nat. λv:Nat.
    λn:Nat.
      if equal n m then <some=v> as OptionalNat
      else t n;
x = case t(5) of
      <none=u> ⇒ 999
    | <some=v> ⇒ v;
```

Enumerations

```
Weekday = <monday:Unit, tuesday:Unit, wednesday:Unit,
           thursday:Unit, friday:Unit>;

nextBusinessDay = λw:Weekday.
  case w of <monday=x>    ⇒ <tuesday=unit> as Weekday
          | <tuesday=x>   ⇒ <wednesday=unit> as Weekday
          | <wednesday=x> ⇒ <thursday=unit> as Weekday
          | <thursday=x>  ⇒ <friday=unit> as Weekday
          | <friday=x>    ⇒ <monday=unit> as Weekday;
```

Terminology: “Union Types”

T_1+T_2 is a disjoint union of T_1 and T_2 (the tags `inl` and `inr` ensure disjointness)

We could also consider a non-disjoint union $T_1 \vee T_2$, but its properties are more complex because it induces an interesting subtype relation...

General Recursion

- In $\lambda_{\rightarrow}$, all programs terminate. (Cf. Chapter 12.)
- Hence, untyped terms like `omega` and `fix` are not typable.
- But we can extend the system with a (typed) fixed-point operator...

Example

```
ff = λie:Nat→Bool.
       λx:Nat.
         if iszero x then true
         else if iszero (pred x) then false
         else ie (pred (pred x));

iseven = fix ff;

iseven 7;
```

New syntactic forms

$\mathtt{t}$	::=	...	terms
		$\mathtt{fix\ t}$	fixed point of t

New evaluation rules

$$\boxed{\mathtt{t} \longrightarrow \mathtt{t}'}$$

$$\begin{array}{c}\mathtt{fix\ (\lambda x{:}T_1.t_2)} \\ \longrightarrow [\mathtt{x} \mapsto \mathtt{(fix\ (\lambda x{:}T_1.t_2))}]\mathtt{t_2}\end{array} \qquad \text{(E-FixBeta)}$$

$$\frac{\mathtt{t_1} \longrightarrow \mathtt{t_1'}}{\mathtt{fix\ t_1} \longrightarrow \mathtt{fix\ t_1'}} \qquad \text{(E-Fix)}$$

New typing rules

$$\boxed{\Gamma \vdash \mathtt{t} : \mathtt{T}}$$

$$\frac{\Gamma \vdash \mathtt{t_1} : \mathtt{T_1} \rightarrow \mathtt{T_1}}{\Gamma \vdash \mathtt{fix}\ \mathtt{t_1} : \mathtt{T_1}} \qquad \text{(T-FIX)}$$

A more convenient form

$$\texttt{letrec x:T}_1\texttt{=t}_1\texttt{ in t}_2 \overset{\text{def}}{=} \texttt{let x = fix (}\lambda\texttt{x:T}_1\texttt{.t}_1\texttt{) in t}_2$$

```
letrec iseven : Nat→Bool =
  λx:Nat.
    if iszero x then true
    else if iszero (pred x) then false
    else iseven (pred (pred x))
in
  iseven 7;
```

Lists

[See book.]

References

Mutability

- In most programming languages, variables are mutable. I.e., a variable provides both
  - a name that refers to a previously calculated value
  - the possibility of overwriting this value with another (which will be referred to by the same name)
- In some languages (e.g., OCaml), these two features are kept separate
  - variables are only for naming — the binding between a variable and its value is immutable
  - introduce a new class of mutable cells or references
  - at any given moment, a reference holds a value (and can be dereferenced to obtain this value)
  - a new value may be assigned to a reference

We choose OCaml's style, which is easier to work with formally.

So a variable of type `T` in most languages (except OCaml) will correspond to a `Ref T` (actually, a `Ref(Option T)`) here.

Examples

[...]

$$\frac{\Gamma \vdash \mathtt{t}_1 : \mathtt{T}_1}{\Gamma \vdash \mathtt{ref}\ \mathtt{t}_1 : \mathtt{Ref}\ \mathtt{T}_1} \qquad \text{(T-Ref)}$$

$$\frac{\Gamma \vdash \mathtt{t}_1 : \mathtt{Ref}\ \mathtt{T}_1}{\Gamma \vdash \mathtt{!t}_1 : \mathtt{T}_1} \qquad \text{(T-Deref)}$$

$$\frac{\Gamma \vdash \mathtt{t}_1 : \mathtt{Ref}\ \mathtt{T}_1 \qquad \Gamma \vdash \mathtt{t}_2 : \mathtt{T}_1}{\Gamma \vdash \mathtt{t}_1 \mathtt{:=} \mathtt{t}_2 : \mathtt{Unit}} \qquad \text{(T-Assign)}$$