CIS 500
Software Foundations
Fall 2006

October 2

Preliminaries

Homework

Results of my email survey:

- There was one badly misdesigned (PhD) problem and a couple of others that were less well thought through than they could have been. These generated the great majority of specific complaints.
- Besides these, most people felt the homeworks were somewhat—but not outrageously—too long.
- People seemed more or less happy with the pace of the course... but no one wanted it faster! :-)
- "PhD questions" are an issue for mixed groups

Homework

Conclusion:

- Basically hold course
- Make homeworks a little shorter and tighter
- Change grading scheme for "PhD problems"
  - Non-PhD students in "PhD groups" will be graded the same as those in non-PhD groups
- Slow down a little more on harder bits of material during lectures
  - I need your help for this!

Midterm

- Wednesday, October 11th
- Topics:
  - Basic OCaml
  - TAPL Chapters 3–9
  - Inductive definitions and proofs
  - Operational semantics
  - Untyped lambda-calculus
  - Simple types

More About Bound Variables

Substitution

Our definition of evaluation is based on the "substitution" of values for free variables within terms.

$$(\lambda x.t_{12})\ v_2 \longrightarrow [x \mapsto v_2]t_{12} \qquad \text{(E-AppAbs)}$$

But what is substitution, exactly? How do we define it?

Substitution

For example, what does

$$(\lambda x.\ x\ (\lambda y.\ x\ y))\ (\lambda x.\ x\ y\ x)$$

reduce to?

Note that this example is not a "complete program" — the whole term is not closed. We are mostly interested in the reduction behavior of closed terms, but reduction of open terms is also important in some contexts:

- program optimization
- alternative reduction strategies such as "full beta-reduction"

Formalizing Substitution

Consider the following definition of substitution:

$$\begin{array}{ll} [x \mapsto s]x = s & \\ [x \mapsto s]y = y & \text{if } x \neq y \\ [x \mapsto s](\lambda y.t_1) = \lambda y.\ ([x \mapsto s]t_1) & \\ [x \mapsto s](t_1\ t_2) = ([x \mapsto s]t_1)([x \mapsto s]t_2) & \end{array}$$

What is wrong with this definition?

Formalizing Substitution

Consider the following definition of substitution:

$$\begin{array}{ll} [x \mapsto s]x = s & \\ [x \mapsto s]y = y & \text{if } x \neq y \\ [x \mapsto s](\lambda y.t_1) = \lambda y.\ ([x \mapsto s]t_1) & \\ [x \mapsto s](t_1\ t_2) = ([x \mapsto s]t_1)([x \mapsto s]t_2) & \end{array}$$

What is wrong with this definition?

It substitutes for free and *bound* variables!

$$[x \mapsto y](\lambda x.\ x) = \lambda x.y$$

This is not what we want!

Substitution, take two

$$\begin{array}{ll} [x \mapsto s]x = s & \\ [x \mapsto s]y = y & \text{if } x \neq y \\ [x \mapsto s](\lambda y.t_1) = \lambda y.\ ([x \mapsto s]t_1) & \text{if } x \neq y \\ [x \mapsto s](\lambda x.t_1) = \lambda x.\ t_1 & \\ [x \mapsto s](t_1\ t_2) = ([x \mapsto s]t_1)([x \mapsto s]t_2) & \end{array}$$

What is wrong with this definition?

Substitution, take two

$$\begin{array}{ll} [x \mapsto s]x = s & \\ [x \mapsto s]y = y & \text{if } x \neq y \\ [x \mapsto s](\lambda y.t_1) = \lambda y.\ ([x \mapsto s]t_1) & \text{if } x \neq y \\ [x \mapsto s](\lambda x.t_1) = \lambda x.\ t_1 & \\ [x \mapsto s](t_1\ t_2) = ([x \mapsto s]t_1)([x \mapsto s]t_2) & \end{array}$$

What is wrong with this definition?

It suffers from *variable capture*!

$$[x \mapsto y](\lambda y.x) = \lambda x.\ x$$

This is also not what we want.

Substitution, take three

$$
\begin{array}{ll}
[x \mapsto s]x = s & \\
[x \mapsto s]y = y & \text{if } x \neq y \\
[x \mapsto s](\lambda y.t_1) = \lambda y.\ ([x \mapsto s]t_1) & \text{if } x \neq y,\ y \notin FV(s) \\
[x \mapsto s](\lambda x.t_1) = \lambda x.\ t_1 & \\
[x \mapsto s](t_1\ t_2) = ([x \mapsto s]t_1)([x \mapsto s]t_2) &
\end{array}
$$

What is wrong with this definition?

Substitution, take three

$$
\begin{array}{ll}
[x \mapsto s]x = s & \\
[x \mapsto s]y = y & \text{if } x \neq y \\
[x \mapsto s](\lambda y.t_1) = \lambda y.\ ([x \mapsto s]t_1) & \text{if } x \neq y,\ y \notin FV(s) \\
[x \mapsto s](\lambda x.t_1) = \lambda x.\ t_1 & \\
[x \mapsto s](t_1\ t_2) = ([x \mapsto s]t_1)([x \mapsto s]t_2) &
\end{array}
$$

What is wrong with this definition?

Now substition is a *partial function!*

E.g., $[x \mapsto y](\lambda y.x)$ is undefined.

But we want an result for every substitution.

Bound variable names shouldn't matter

It's annoying that that the "spelling" of bound variable names is causing trouble with our definition of substitution.

Intuition tells us that there shouldn't be a difference between the functions $\lambda x.x$ and $\lambda y.y$. Both of these functions do exactly the same thing.

Because they differ only in the names of their bound variables, we'd like to think that these *are* the same function.

We call such terms *alpha-equivalent*.

Alpha-equivalence classes

In fact, we can create equivalence classes of terms that differ only in the names of bound variables.

When working with the lambda calculus, it is convenient to think about these *equivalence classes*, instead of raw terms.

For example, when we write $\lambda x.x$ we mean not just this term, but the class of terms that includes $\lambda y.y$ and $\lambda z.z$.

We can now freely choose a different *representative* from a term's alpha-equivalence class, whenever we need to, to avoid getting stuck.

Substitution, for alpha-equivalence classes

Now consider substitution as an operation over *alpha-equivalence classes* of terms.

$$
\begin{array}{ll}
[x \mapsto s]x = s & \\
[x \mapsto s]y = y & \text{if } x \neq y \\
[x \mapsto s](\lambda y.t_1) = \lambda y.\ ([x \mapsto s]t_1) & \text{if } x \neq y,\ y \notin FV(s) \\
[x \mapsto s](\lambda x.t_1) = \lambda x.\ t_1 & \\
[x \mapsto s](t_1\ t_2) = ([x \mapsto s]t_1)([x \mapsto s]t_2) &
\end{array}
$$

Examples:

- $[x \mapsto y](\lambda y.x)$ must give the same result as $[x \mapsto y](\lambda z.x)$. We know the latter is $\lambda z.y$, so that is what we will use for the former.
- $[x \mapsto y](\lambda x.z)$ must give the same result as $[x \mapsto y](\lambda w.z)$. We know the latter is $\lambda w.z$ so that is what we use for the former.

Review

So what does

$$(\lambda x.\ x\ (\lambda y.\ x\ y))\ (\lambda x.\ x\ y\ x)$$

reduce to?

Types

Plan

- For today, we'll go back to the simple language of arithmetic and boolean expressions and show how to equip it with a (very simple) type system
- The key property of this type system will be *soundness*: Well-typed programs do not get stuck
- Next time, we'll develop a simple type system for the lambda-calculus
- We'll spend a good part of the rest of the semester adding features to this type system

Outline

1. begin with a set of terms, a set of values, and an evaluation relation
2. define a set of *types* classifying values according to their "shapes"
3. define a *typing relation* `t : T` that classifies terms according to the shape of the values that result from evaluating them
4. check that the typing relation is *sound* in the sense that,
   4.1 if `t : T` and $t \longrightarrow^* v$, then `v : T`
   4.2 if `t : T`, then evaluation of `t` will not get stuck

Review: Arithmetic Expressions – Syntax

`t ::=`		*terms*
	`true`	*constant true*
	`false`	*constant false*
	`if t then t else t`	*conditional*
	`0`	*constant zero*
	`succ t`	*successor*
	`pred t`	*predecessor*
	`iszero t`	*zero test*
`v ::=`		*values*
	`true`	*true value*
	`false`	*false value*
	`nv`	*numeric value*
`nv ::=`		*numeric values*
	`0`	*zero value*
	`succ nv`	*successor value*

Evaluation Rules

$$\texttt{if true then } t_2 \texttt{ else } t_3 \longrightarrow t_2 \qquad \text{(E-IfTrue)}$$

$$\texttt{if false then } t_2 \texttt{ else } t_3 \longrightarrow t_3 \qquad \text{(E-IfFalse)}$$

$$\frac{t_1 \longrightarrow t_1'}{\texttt{if } t_1 \texttt{ then } t_2 \texttt{ else } t_3 \longrightarrow \texttt{if } t_1' \texttt{ then } t_2 \texttt{ else } t_3} \qquad \text{(E-If)}$$

$$\frac{t_1 \longrightarrow t_1'}{\texttt{succ } t_1 \longrightarrow \texttt{succ } t_1'} \qquad \text{(E-Succ)}$$

$$\texttt{pred } 0 \longrightarrow 0 \qquad \text{(E-PredZero)}$$

$$\texttt{pred (succ } nv_1\texttt{)} \longrightarrow nv_1 \qquad \text{(E-PredSucc)}$$

$$\frac{t_1 \longrightarrow t_1'}{\texttt{pred } t_1 \longrightarrow \texttt{pred } t_1'} \qquad \text{(E-Pred)}$$

$$\texttt{iszero } 0 \longrightarrow \texttt{true} \qquad \text{(E-IszeroZero)}$$

$$\texttt{iszero (succ } nv_1\texttt{)} \longrightarrow \texttt{false} \qquad \text{(E-IszeroSucc)}$$

$$\frac{t_1 \longrightarrow t_1'}{\texttt{iszero } t_1 \longrightarrow \texttt{iszero } t_1'} \qquad \text{(E-IsZero)}$$

Types

In this language, values have two possible "shapes": they are either booleans or numbers.

$\mathtt{T}$ ::=		*types*
	$\mathtt{Bool}$	*type of booleans*
	$\mathtt{Nat}$	*type of numbers*

Typing Rules

$$\mathtt{true} : \mathtt{Bool} \qquad \text{(T-True)}$$

$$\mathtt{false} : \mathtt{Bool} \qquad \text{(T-False)}$$

$$\frac{\mathtt{t}_1 : \mathtt{Bool} \quad \mathtt{t}_2 : \mathtt{T} \quad \mathtt{t}_3 : \mathtt{T}}{\mathtt{if}\ \mathtt{t}_1\ \mathtt{then}\ \mathtt{t}_2\ \mathtt{else}\ \mathtt{t}_3 : \mathtt{T}} \qquad \text{(T-If)}$$

$$\mathtt{0} : \mathtt{Nat} \qquad \text{(T-Zero)}$$

$$\frac{\mathtt{t}_1 : \mathtt{Nat}}{\mathtt{succ}\ \mathtt{t}_1 : \mathtt{Nat}} \qquad \text{(T-Succ)}$$

$$\frac{\mathtt{t}_1 : \mathtt{Nat}}{\mathtt{pred}\ \mathtt{t}_1 : \mathtt{Nat}} \qquad \text{(T-Pred)}$$

$$\frac{\mathtt{t}_1 : \mathtt{Nat}}{\mathtt{iszero}\ \mathtt{t}_1 : \mathtt{Bool}} \qquad \text{(T-IsZero)}$$

Typing Derivations

Every pair $(\mathtt{t}, \mathtt{T})$ in the typing relation can be justified by a *derivation tree* built from instances of the inference rules.

$$\dfrac{\dfrac{\dfrac{}{\mathtt{0} : \mathtt{Nat}}\text{T-Zero}}{\mathtt{iszero}\ \mathtt{0} : \mathtt{Bool}}\text{T-IsZero} \quad \dfrac{}{\mathtt{0} : \mathtt{Nat}}\text{T-Zero} \quad \dfrac{\dfrac{}{\mathtt{0} : \mathtt{Nat}}\text{T-Zero}}{\mathtt{pred}\ \mathtt{0} : \mathtt{Nat}}\text{T-Pred}}{\mathtt{if}\ \mathtt{iszero}\ \mathtt{0}\ \mathtt{then}\ \mathtt{0}\ \mathtt{else}\ \mathtt{pred}\ \mathtt{0} : \mathtt{Nat}}\text{T-If}$$

Proofs of properties about the typing relation often proceed by induction on typing derivations.

Imprecision of Typing

Like other static program analyses, type systems are generally *imprecise*: they do not predict exactly what kind of value will be returned by every program, but just a conservative (safe) approximation.

$$\frac{\mathtt{t}_1 : \mathtt{Bool} \quad \mathtt{t}_2 : \mathtt{T} \quad \mathtt{t}_3 : \mathtt{T}}{\mathtt{if}\ \mathtt{t}_1\ \mathtt{then}\ \mathtt{t}_2\ \mathtt{else}\ \mathtt{t}_3 : \mathtt{T}} \qquad \text{(T-If)}$$

Using this rule, we cannot assign a type to

```
if true then 0 else false
```

even though this term will certainly evaluate to a number.

Properties of the Typing Relation

Type Safety

The safety (or soundness) of this type system can be expressed by two properties:

1. *Progress:* A well-typed term is not stuck

   If $t : T$, then either t is a value or else $t \longrightarrow t'$ for some t'.

2. *Preservation:* Types are preserved by one-step evaluation

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

Inversion

Lemma:

1. If $\mathtt{true} : \mathtt{R}$, then $\mathtt{R} = \mathtt{Bool}$.
2. If $\mathtt{false} : \mathtt{R}$, then $\mathtt{R} = \mathtt{Bool}$.
3. If $\mathtt{if}\ \mathtt{t}_1\ \mathtt{then}\ \mathtt{t}_2\ \mathtt{else}\ \mathtt{t}_3 : \mathtt{R}$, then $\mathtt{t}_1 : \mathtt{Bool}$, $\mathtt{t}_2 : \mathtt{R}$, and $\mathtt{t}_3 : \mathtt{R}$.
4. If $\mathtt{0} : \mathtt{R}$, then $\mathtt{R} = \mathtt{Nat}$.
5. If $\mathtt{succ}\ \mathtt{t}_1 : \mathtt{R}$, then $\mathtt{R} = \mathtt{Nat}$ and $\mathtt{t}_1 : \mathtt{Nat}$.
6. If $\mathtt{pred}\ \mathtt{t}_1 : \mathtt{R}$, then $\mathtt{R} = \mathtt{Nat}$ and $\mathtt{t}_1 : \mathtt{Nat}$.
7. If $\mathtt{iszero}\ \mathtt{t}_1 : \mathtt{R}$, then $\mathtt{R} = \mathtt{Bool}$ and $\mathtt{t}_1 : \mathtt{Nat}$.

Inversion

Lemma:

1. If $\mathtt{true} : \mathtt{R}$, then $\mathtt{R} = \mathtt{Bool}$.
2. If $\mathtt{false} : \mathtt{R}$, then $\mathtt{R} = \mathtt{Bool}$.
3. If $\mathtt{if}\ \mathtt{t}_1\ \mathtt{then}\ \mathtt{t}_2\ \mathtt{else}\ \mathtt{t}_3 : \mathtt{R}$, then $\mathtt{t}_1 : \mathtt{Bool}$, $\mathtt{t}_2 : \mathtt{R}$, and $\mathtt{t}_3 : \mathtt{R}$.
4. If $\mathtt{0} : \mathtt{R}$, then $\mathtt{R} = \mathtt{Nat}$.
5. If $\mathtt{succ}\ \mathtt{t}_1 : \mathtt{R}$, then $\mathtt{R} = \mathtt{Nat}$ and $\mathtt{t}_1 : \mathtt{Nat}$.
6. If $\mathtt{pred}\ \mathtt{t}_1 : \mathtt{R}$, then $\mathtt{R} = \mathtt{Nat}$ and $\mathtt{t}_1 : \mathtt{Nat}$.
7. If $\mathtt{iszero}\ \mathtt{t}_1 : \mathtt{R}$, then $\mathtt{R} = \mathtt{Bool}$ and $\mathtt{t}_1 : \mathtt{Nat}$.

Proof: ...

Inversion

Lemma:

1. If $\mathtt{true} : \mathtt{R}$, then $\mathtt{R} = \mathtt{Bool}$.
2. If $\mathtt{false} : \mathtt{R}$, then $\mathtt{R} = \mathtt{Bool}$.
3. If $\mathtt{if}\ \mathtt{t}_1\ \mathtt{then}\ \mathtt{t}_2\ \mathtt{else}\ \mathtt{t}_3 : \mathtt{R}$, then $\mathtt{t}_1 : \mathtt{Bool}$, $\mathtt{t}_2 : \mathtt{R}$, and $\mathtt{t}_3 : \mathtt{R}$.
4. If $\mathtt{0} : \mathtt{R}$, then $\mathtt{R} = \mathtt{Nat}$.
5. If $\mathtt{succ}\ \mathtt{t}_1 : \mathtt{R}$, then $\mathtt{R} = \mathtt{Nat}$ and $\mathtt{t}_1 : \mathtt{Nat}$.
6. If $\mathtt{pred}\ \mathtt{t}_1 : \mathtt{R}$, then $\mathtt{R} = \mathtt{Nat}$ and $\mathtt{t}_1 : \mathtt{Nat}$.
7. If $\mathtt{iszero}\ \mathtt{t}_1 : \mathtt{R}$, then $\mathtt{R} = \mathtt{Bool}$ and $\mathtt{t}_1 : \mathtt{Nat}$.

Proof: ...

This leads directly to a recursive algorithm for calculating the type of a term...

Typechecking Algorithm

```
typeof(t) = if t = true then Bool
            else if t = false then Bool
            else if t = if t1 then t2 else t3 then
              let T1 = typeof(t1) in
              let T2 = typeof(t2) in
              let T3 = typeof(t3) in
              if T1 = Bool and T2=T3 then T2
              else "not typable"
            else if t = 0 then Nat
            else if t = succ t1 then
              let T1 = typeof(t1) in
              if T1 = Nat then Nat else "not typable"
            else if t = pred t1 then
              let T1 = typeof(t1) in
              if T1 = Nat then Nat else "not typable"
            else if t = iszero t1 then
              let T1 = typeof(t1) in
              if T1 = Nat then Bool else "not typable"
```

Canonical Forms

Lemma:

1. If $\mathtt{v}$ is a value of type $\mathtt{Bool}$, then $\mathtt{v}$ is either $\mathtt{true}$ or $\mathtt{false}$.
2. If $\mathtt{v}$ is a value of type $\mathtt{Nat}$, then $\mathtt{v}$ is a numeric value.

Canonical Forms

Lemma:

1. If $\mathtt{v}$ is a value of type $\mathtt{Bool}$, then $\mathtt{v}$ is either $\mathtt{true}$ or $\mathtt{false}$.
2. If $\mathtt{v}$ is a value of type $\mathtt{Nat}$, then $\mathtt{v}$ is a numeric value.

Proof: ...

Progress

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

Progress

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

Proof:

Progress

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

Proof: By induction on a derivation of $\mathtt{t : T}$.

Progress

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

Proof: By induction on a derivation of $\mathtt{t : T}$.

The T-True, T-False, and T-Zero cases are immediate, since $\mathtt{t}$ in these cases is a value.

Progress

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

Proof: By induction on a derivation of $\mathtt{t : T}$.

The T-True, T-False, and T-Zero cases are immediate, since $\mathtt{t}$ in these cases is a value.

Case T-If: $\mathtt{t} = \mathtt{if\ t_1\ then\ t_2\ else\ t_3}$
$\mathtt{t_1 : Bool} \quad \mathtt{t_2 : T} \quad \mathtt{t_3 : T}$

Progress

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

Proof: By induction on a derivation of $\mathtt{t : T}$.

The T-True, T-False, and T-Zero cases are immediate, since $\mathtt{t}$ in these cases is a value.

Case T-If: $\mathtt{t} = \mathtt{if\ t_1\ then\ t_2\ else\ t_3}$
$\mathtt{t_1 : Bool} \quad \mathtt{t_2 : T} \quad \mathtt{t_3 : T}$

By the induction hypothesis, either $\mathtt{t_1}$ is a value or else there is some $\mathtt{t}_1'$ such that $\mathtt{t_1} \longrightarrow \mathtt{t}_1'$. If $\mathtt{t_1}$ is a value, then the canonical forms lemma tells us that it must be either $\mathtt{true}$ or $\mathtt{false}$, in which case either E-IfTrue or E-IfFalse applies to $\mathtt{t}$. On the other hand, if $\mathtt{t_1} \longrightarrow \mathtt{t}_1'$, then, by E-If, $\mathtt{t} \longrightarrow \mathtt{if\ t_1'\ then\ t_2\ else\ t_3}$.

Preservation

Theorem: If $\mathtt{t} : \mathtt{T}$ and $\mathtt{t} \longrightarrow \mathtt{t}'$, then $\mathtt{t}' : \mathtt{T}$.

Preservation

Theorem: If $\mathtt{t} : \mathtt{T}$ and $\mathtt{t} \longrightarrow \mathtt{t}'$, then $\mathtt{t}' : \mathtt{T}$.

Proof: ...

Recap: Type Systems

- Very successful example of a *lightweight formal method*
- big topic in PL research
- enabling technology for all sorts of other things, e.g. language-based security
- the skeleton around which modern programming languages are designed