Lesson 1
Untyped Arithmetic Expressions

1/4/05

Topics

- abstract syntax
- inductive definitions and proofs
- evaluation
- modeling runtime errors

An abstract syntax

```
t ::=
      true
      false
      if t then t else t
      0
      succ t
      pred t
      iszero t
```

Terms defined by a BNF style grammar.
Not worried about ambiguity.
t is a syntactic metavariable

example terms

```
true

0

succ 0

if false then 0
   else pred(if true then succ 0 else 0)

iszero true

if 0 then true else pred 0
```

Inductive defn of terms

Defn: The set of terms is the smallest set $\mathcal{T}$ such that

1. {true, false, 0} $\subseteq \mathcal{T}$

2. if t $\in \mathcal{T}$, then {**succ** t, **pred** t, **iszero** t} $\subseteq \mathcal{T}$

3. if t1, t2, t3 $\in \mathcal{T}$, then **if** t1 **then** t2 **else** t3 $\in \mathcal{T}$

Terms defined using inference rules

Defn: The set of terms is defined by the following rules:

$$\texttt{true} \in \mathcal{T} \qquad \texttt{false} \in \mathcal{T} \qquad \texttt{0} \in \mathcal{T}$$

$$\frac{t \in \mathcal{T}}{\texttt{succ t} \in \mathcal{T}} \qquad \frac{t \in \mathcal{T}}{\texttt{pred t} \in \mathcal{T}} \qquad \frac{t \in \mathcal{T}}{\texttt{iszero t} \in \mathcal{T}}$$

$$\frac{t1 \in \mathcal{T} \qquad t2 \in \mathcal{T} \qquad t3 \in \mathcal{T}}{\text{if } t1 \text{ then } t2 \text{ else } t3 \in \mathcal{T}}$$

Definition by induction, concretely

Defn: For each i, define S(i) as follows

$\mathcal{S}(0) = \varnothing$

$\mathcal{S}(i+1) = \{\text{true, false, 0}\}$

$\cup \{\text{succ t, pred t, iszero t} \mid \text{t} \in \mathcal{S}(i)\}$

$\cup \{\text{if t1 then t2 else t3} \mid \text{t1,t2,t3} \in \mathcal{S}(i)\}$

Then let

$\mathcal{S} = \bigcup \{\mathcal{S}(i) \mid i \in \text{Nat}\}$

Proposition: $\mathcal{S} = \mathcal{T}$

Defining functions inductively

Constants appearing in a term

```
consts(true) = {true}
consts(false) = {false}
consts(0) = {0}
consts(succ t) = consts(t)
consts(pred t) = consts(t)
consts(iszero t) = consts(t)
consts(if t1 then t2 else t3) =
  consts(t1)∪ consts(t1)∪ consts(t1)
```

Defining functions inductively

Size of a term:

```
size(true) = 1
size(false) = 1
size(0) = 1
size(succ t) = size(t) + 1
size(pred t) = size(t) + 1
size(iszero t) = size(t) + 1
size(if t1 then t2 else t3) =
  size(t1) + size(t1) + size(t1) + 1
```

Defining functions inductively

Depth of a term

```
depth(true) = 1
depth(false) = 1
depth(0) = 1
depth(succ t) = depth(t) + 1
depth(pred t) = depth(t) + 1
depth(iszero t) = depth(t) + 1
depth(if t1 then t2 else t3) =
  max(depth(t1),depth(t1),depth(t1)) + 1
```

Proof by induction (on depth)

If, for each term s,
given P(r) for all terms with
depth(r) < depth(s),
we can show P(s)
then P(s) holds for all terms.

Proof by induction (on size)

If, for each term s,
  given P(r) for all terms with
    size(r) < size(s),
  we can show P(s)
then P(s) holds for all terms.

Proof by structural induction

If, for each term s,
  given P(r) for all immediate
  subterms of S,
  we can show P(s)
then P(s) holds for all terms.

Operational semantics

An abstract machine for with instructions on how to evaluate terms of the language.

In simple cases, the terms of the language can be interpretedas the instructions.

The values (results) can also be taken to be (simple) terms in the language.

Evaluation: booleans

Terms

t ::= **true**

| **false**

| **if** t **then** t **else** t

Values

v ::= **true**

| **false**

Evaluation (reduction) relation

An evaluation relation is a binary relation

$$t \rightarrow t'$$

on terms representing one step of evaluation.
This is known as a small-step or one-step evaluation relation. (Also known as a transition relation.)

A normal form is a term which is fully evaluated, i.e. for which no further evaluation is possible.
Thus, t is a normal form term if there is no term t′ such that $t \rightarrow t'$.

Evaluation rules for boolean terms

The evaluation releation t → t′ is the least relation satisfying the following rules.

```
if true then t2 else t3 →  t2

if false then t2 else t3 →  t3

        t1 →  t1′
-------------------------------
if t1 then t2 else t3 →
   if t1′ then t2 else t3
```

Evaluation strategy

Evaluation rules can determine an evaluation strategy that limits where evaluation takes place.

Example:

if true then (if false then false else true) else true

$\rightarrow$ if false then false else true

But not

if true then (if false then false else true) else true

$\rightarrow$ if true then true else true

Determinacy

Evalution of boolean terms is deterministic. That is if $t \rightarrow t'$ and $t \rightarrow t''$, then $t' = t''$.

Proof by induction on derivations of $t \rightarrow t'$.

Values and normal forms

Every value is a normal form (is in normal form).

For booleans, every normal form is a value.

But generally, not all normal forms are values.

E.g. pred(true)

Such non-value normal forms are called stuck.

Multistep evaluation

Defn: Let $\rightarrow^*$ be the reflexive, transitive closure of $\rightarrow$. I.e $\rightarrow^*$ is the least relation such that

(1) if $t \rightarrow t'$ then $t \rightarrow^* t'$

(2) $t \rightarrow^* t$

(3) if $t \rightarrow^* t'$ and $t' \rightarrow^* t''$ then $t \rightarrow^* t''$

Boolean normal forms

Uniqueness of normal forms

Theorem: If $t \to^* u$ and $t \to^* u'$ where u and u' are normal forms, then $u = u'$.

Proof: determinacy of $\to$

Existence of normal forms

Theorem: For any term t, there is a normal form u such that $t \to^* u$.

Proof: If $t \to t'$, then t' is smaller than t, i.e. $size(t') < size(t)$.

Evaluation for arithmetic

Terms

t ::= ... | 0 | succ t | pred t | iszero t

Values

v ::= ... | nv

nv ::= 0 | succ nv

Base computation rules

pred 0 → 0	E-PredZero
pred (succ nv) → nv	E-PredSucc
iszero 0 → true	E-IszeroZero
iszero (succ nv) → false	E-IszeroSucc

Note that the E-PredSucc and E-IsZeroSucc rules are restricted to the case where the argument is a value (call-by-value).

Congruence rules (or Search rules)

$$\frac{t \rightarrow t'}{\text{succ } t \rightarrow \text{succ } t'}$$

E-Succ

$$\frac{t \rightarrow t'}{\text{pred } t \rightarrow \text{pred } t'}$$

E-Pred

$$\frac{t \rightarrow t'}{\text{iszero } t \rightarrow \text{iszero } t'}$$

E-Iszero

Homework 1

- Do exercises 3.5.13 and 3.5.14.

Stuck terms and runtime errors

Stuck terms

Defn: a closed term is stuck if it is a normal form but is not a value.

Examples:

pred true

if succ(0) then true else false

We can take stuck terms as representing runtime errors.