Untyped Arithmetic Expressions

Harley Eades

Syntax

$$
\begin{aligned}
t ::= \\
& \mid \text{true} \\
& \mid \text{false} \\
& \mid \text{if } t \text{ then } t \text{ else } t \\
& \mid 0 \\
& \mid \text{succ } t \\
& \mid \text{pred } t \\
& \mid \text{iszero } t
\end{aligned}
$$

Syntax

$t ::=$

| true
| false
| if t then t else t
| 0 — zero
| succ t — successor
| pred t — predecessor
| iszero t — zero test

Unary Natural Numbers

n	p
0	0
1	succ 0
2	succ succ 0
3	succ succ succ 0
$\vdots$	$\vdots$
n	$\text{succ}^n\ 0$

Unary Natural Numbers

Predecessor

$$\mathsf{pred}\,0 = 0$$
$$\mathsf{pred}\,(\mathsf{succ}\,n) = n$$

Unary Natural Numbers

Zero Test

$$\mathsf{iszero}\,0 = \mathsf{true}$$
$$\mathsf{iszero}\,(\mathsf{succ}\,n) = \mathsf{false}$$

Exercise

How do we define addition?

$$\text{add}\, p_1\, p_2 = \,?$$

Exercise

How do we define addition?

$$\mathsf{add}\, 0\, p_2 = p_2$$
$$\mathsf{add}\, (\mathsf{succ}\, p_1)\, p_2 = \mathsf{succ}\, (\mathsf{add}\, p_1\, p_2)$$

Exercise

How do we define subtraction?

$$\mathsf{sub}\, p_1\, p_2 = 0$$

Exercise

How do we define subtraction?

$$\mathsf{sub}\, p_1\, 0 = p_1$$
$$\mathsf{sub}\, p_1\, (\mathsf{succ}\, p_2) = \mathsf{pred}\, p_1$$

Exercise

How do we define multiplication?

$$\mathsf{mult}\; p_1\, p_2 = \;?$$

Exercise

How do we define multiplication?

$$\mathsf{mult}\,0\,p_2 = 0$$
$$\mathsf{mult}\,(\mathsf{succ}\,0)\,p_2 = p_2$$
$$\mathsf{mult}\,(\mathsf{succ}\,p_1)\,p_2 = \mathsf{add}\,(\mathsf{mult}\,p_1\,p_2)\,p_2$$

Terms

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

We call the programs generated by t terms.

Terms

Definition: The set of <u>terms</u> is the smallest set $\mathscr{T}$ such that:

1. $\{\text{true}, \text{false}\} \subseteq \mathscr{T}$;
2. if $t \in \mathscr{T}$, then $\{\text{succ}\ t, \text{pred}\ t\ \text{iszero}\ t\} \subseteq \mathscr{T}$;
3. if $\{t_1, t_2, t_3\} \subseteq \mathscr{T}$, then $\text{if}\ t_1\ \text{then}\ t_2\ \text{else}\ t_3 \in \mathscr{T}$

Terms

An inductive definition

Definition: The set of terms is the smallest set $\mathscr{T}$ such that:

1. $\{\text{true}, \text{false}\} \subseteq \mathscr{T}$;
2. if $t \in \mathscr{T}$, then $\{\text{succ}\ t, \text{pred}\ t\ \text{iszero}\ t\} \subseteq \mathscr{T}$;
3. if $\{t_1, t_2, t_3\} \subseteq \mathscr{T}$, then $\text{if}\ t_1\ \text{then}\ t_2\ \text{else}\ t_3 \in \mathscr{T}$

Terms

<u>Smallest Set</u>: For every other set, $\mathscr{T}'$, satisfying conditions 1-3, it is the case that $\mathscr{T} \subseteq \mathscr{T}'$.

Definition: The set of <u>terms</u> is the smallest set $\mathscr{T}$ such that:

1. $\{\text{true}, \text{false}\} \subseteq \mathscr{T}$;
2. if $t \in \mathscr{T}$, then $\{\text{succ}\, t, \text{pred}\, t\, \text{iszero}\, t\} \subseteq \mathscr{T}$;
3. if $\{t_1, t_2, t_3\} \subseteq \mathscr{T}$, then $\text{if}\, t_1\, \text{then}\, t_2\, \text{else}\, t_3 \in \mathscr{T}$

Inductive Definitions

- A judgment is some predicate.
- Inference rules define when a judgment $\mathcal{J}$ is true.
- Given a judgment $\mathcal{J}'$, we show that $\mathcal{J}'$ holds by giving a derivation tree of the inference rules that begins with $\mathcal{J}'$ and all branches end with axoims.

Inference Rules

Axiom

$$\frac{}{\mathscr{J}}\,\text{Name}$$

Compound

$$\frac{\mathscr{J}_1 \quad \cdots \quad \mathscr{J}_i}{\mathscr{J}}\,\text{Name}$$

Inference Rules

Axiom

$$\frac{}{\mathscr{J}}\ \text{Name}$$

Compound

$$\frac{\mathscr{J}_1 \quad \cdots \quad \mathscr{J}_i}{\mathscr{J}}\ \text{Name}$$

if $\mathscr{J}_1 \wedge \cdots \wedge \mathscr{J}_i$, then $\mathscr{J}$

Inductive Definition of Terms

$\underline{t \in \mathcal{T}}$ is our judgment defined by:

$$\frac{}{\text{true} \in \mathcal{T}}\;\text{T} \qquad \frac{t_1 \in \mathcal{T}}{\text{succ}\; t_1 \in \mathcal{T}}\;\text{succ}$$

$$\frac{}{\text{false} \in \mathcal{T}}\;\text{F} \qquad \frac{t_1 \in \mathcal{T}}{\text{pred}\; t_1 \in \mathcal{T}}\;\text{pred} \qquad \frac{t_1 \in \mathcal{T} \quad t_2 \in \mathcal{T} \quad t_3 \in \mathcal{T}}{\text{if}\; t_1 \;\text{then}\; t_2 \;\text{else}\; t_3 \in \mathcal{T}}\;\text{if}$$

$$\frac{}{0 \in \mathcal{T}}\;\text{0} \qquad \frac{t_1 \in \mathcal{T}}{\text{iszero}\; t_1 \in \mathcal{T}}\;\text{iszero}$$

Inductive Definition: Derivations

Goal Directed Proof

Start with what you're trying to prove, the goal, and then reduce it into one or more subgoals; repeat this process on each subgoal until all subgoals reduce to axioms.

Inductive Definition: Derivations

All our goals will be judgments. Suppose $\mathscr{J}$ is some judgment. Then we derive $\mathscr{J}$ using the inference rules defining when judgments of the form of $\mathscr{J}$ hold using a derivation tree.

Inductive Definition: Derivations

We call $\mathscr{D}$ as <u>derivation tree</u> of judgment $\mathscr{J}$ if:

1. $\mathscr{D}$ is an axiom whose conclusion matches $\mathscr{J}$;
2. $\mathscr{D}$ has the form:

$$\frac{\mathscr{D}_1 \quad \cdots \quad \mathscr{D}_i}{\mathscr{J}}\ \text{Name}$$

where $\mathscr{D}_1, \ldots, \mathscr{D}_i$ are derivation trees and "Name" is one of the inference rules of $\mathscr{J}$ where the premises match the conclusions of $\mathscr{D}_1, \ldots, \mathscr{D}_i$ respectively.

Inductive Definition of Terms

$\underline{t \in \mathscr{T}}$ is our judgment defined by:

$$\frac{}{\text{true} \in \mathscr{T}}\ \text{T} \qquad \frac{t_1 \in \mathscr{T}}{\text{succ}\ t_1 \in \mathscr{T}}\ \text{succ}$$

$$\frac{}{\text{false} \in \mathscr{T}}\ \text{F} \qquad \frac{t_1 \in \mathscr{T}}{\text{pred}\ t_1 \in \mathscr{T}}\ \text{pred} \qquad \frac{t_1 \in \mathscr{T} \quad t_2 \in \mathscr{T} \quad t_3 \in \mathscr{T}}{\text{if}\ t_1\ \text{then}\ t_2\ \text{else}\ t_3 \in \mathscr{T}}\ \text{if}$$

$$\frac{}{0 \in \mathscr{T}}\ 0 \qquad \frac{t_1 \in \mathscr{T}}{\text{iszero}\ t_1 \in \mathscr{T}}\ \text{iszero}$$

Inductive Definition of Terms

$\mathsf{if\ iszero}\ 0\ \mathsf{then\ true\ else\ false} \in \mathscr{T}$

Inductive Definition of Terms

$$\frac{\text{iszero} \in \mathscr{T} \qquad \text{true} \in \mathscr{T} \qquad \text{false} \in \mathscr{T}}{\text{if iszero } 0 \text{ then true else false} \in \mathscr{T}}\ \text{if}$$

Inductive Definition of Terms

$$
\dfrac{\dfrac{0 \in \mathscr{T}}{\text{iszero}\ 0 \in \mathscr{T}}\,\text{iszero} \qquad \text{true} \in \mathscr{T} \qquad \text{false} \in \mathscr{T}}{\text{if iszero}\ 0\ \text{then true else false} \in \mathscr{T}}\,\text{if}
$$

Inductive Definition of Terms

$$
\dfrac{\dfrac{\dfrac{}{0 \in \mathscr{T}}\,\textsf{0}}{\text{iszero}\ 0 \in \mathscr{T}}\,\textsf{iszero} \qquad \text{true} \in \mathscr{T} \qquad \text{false} \in \mathscr{T}}{\text{if iszero}\ 0\ \text{then true else false} \in \mathscr{T}}\,\textsf{if}
$$

Inductive Definition of Terms

$$\dfrac{\dfrac{\dfrac{}{0 \in \mathscr{T}}\;\mathsf{0}}{\text{iszero}\ 0 \in \mathscr{T}}\;\mathsf{iszero} \qquad \dfrac{}{\text{true} \in \mathscr{T}}\;\mathsf{true} \qquad \text{false} \in \mathscr{T}}{\text{if iszero}\ 0\ \text{then true else false} \in \mathscr{T}}\;\mathsf{if}$$

Derivations using Terms

$$
\dfrac{\dfrac{\dfrac{}{0 \in \mathscr{T}}\,\text{0}}{\text{iszero}\, 0 \in \mathscr{T}}\,\text{iszero} \qquad \dfrac{}{\text{true} \in \mathscr{T}}\,\text{true} \qquad \dfrac{}{\text{false} \in \mathscr{T}}\,\text{false}}{\text{if iszero}\, 0 \text{ then true else false} \in \mathscr{T}}\,\text{if}
$$

Exercise

Suppose our judgment is

$$t \in \mathscr{T}_{\mathbb{N}}$$

where $\mathscr{T}_{\mathbb{N}}$ is the subset of terms corresponding to the natural numbers.

i. Define inference rules for when this judgment holds.
ii. Derive: $\text{succ pred succ } 0 \in \mathscr{T}_{\mathbb{N}}$

Induction on Terms

What can we say about t if we know $t \in \mathscr{T}$?

Induction on Terms

What can we say about t if we know $t \in \mathscr{T}$?

1. t is a constant

Induction on Terms

What can we say about t if we know $t \in \mathscr{T}$?

1. t is a constant; or
2. $t \in \{\text{succ}\, t_1, \text{pred}\, t_1, \text{iszero}\, t_1\}$ for some smaller term t_1

Induction on Terms

What can we say about t if we know $t \in \mathscr{T}$?

1. t is a constant; or
2. $t \in \{\text{succ}\, t_1, \text{pred}\, t_1, \text{iszero}\, t_1\}$ for some smaller term t_1; or
3. $t = \text{if}\, t_1, \text{then}\, t_2\, \text{else}\, t_3$ for some smaller terms t_1, t_2, t_3.

Induction on Terms

This is an important reasoning principle!

1. Inductive definitions of functions.
2. Inductive proofs.

What can we say about t if we know $t \in \mathcal{T}$?

1. t is a constant; or
2. $t \in \{\text{succ}\, t_1, \text{pred}\, t_1, \text{iszero}\, t_1\}$ for some smaller term t_1; or
3. $t = \text{if}\, t_1\, \text{then}\, t_2\, \text{else}\, t_3$ for some smaller terms t_1, t_2, t_3.

Inductive Definition of Functions

$$
\begin{aligned}
\mathit{const}(\mathsf{true}) &= \{\mathsf{true}\} \\
\mathit{const}(\mathsf{false}) &= \{\mathsf{false}\} \\
\mathit{const}(0) &= \{0\} \\
\mathit{const}(\mathsf{succ}(t)) &= \mathit{const}(t) \\
\mathit{const}(\mathsf{pred}(t)) &= \mathit{const}(t) \\
\mathit{const}(\mathsf{iszero}(t)) &= \mathit{const}(t) \\
\mathit{const}(\mathsf{if}\ t_1\ \mathsf{then}\ t_2\ \mathsf{else}\ t_3) &= \mathit{const}(t_1) \cup \mathit{const}(t_2) \cup \mathit{const}(t_3)
\end{aligned}
$$

Inductive Definition of Functions

$$
\begin{aligned}
size(\mathsf{true}) &= 1 \\
size(\mathsf{false}) &= 1 \\
size(0) &= 1 \\
size(\mathsf{succ}(t)) &= size(t) + 1 \\
size(\mathsf{pred}(t)) &= size(t) + 1 \\
size(\mathsf{iszero}(t)) &= size(t) + 1 \\
size(\mathsf{if}\ t_1\ \mathsf{then}\ t_2\ \mathsf{else}\ t_3) &= size(t_1) + size(t_2) + size(t_3) + 1
\end{aligned}
$$

Inductive Definition of Functions

$$
\begin{aligned}
depth(\mathsf{true}) &= 1 \\
depth(\mathsf{false}) &= 1 \\
depth(0) &= 1 \\
depth(\mathsf{succ}(t)) &= depth(t) + 1 \\
depth(\mathsf{pred}(t)) &= depth(t) + 1 \\
depth(\mathsf{iszero}(t)) &= depth(t) + 1 \\
depth(\mathsf{if}\ t_1\ \mathsf{then}\ t_2\ \mathsf{else}\ t_3) &= max(depth(t_1), depth(t_2), depth(t_3))
\end{aligned}
$$

Principles of Induction on Terms

<u>Depth</u> gives an induction principle for reasoning about terms:

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

Principles of Induction on Terms

Suppose we know for every subterm t' of a term t, $size(t') < size(t)$.

Lemma. For every $t \in \mathcal{T}$, $|const(t)| \leq size(t)$

Proof. By induction on the depth of t. There are three cases to consider.

1. t is a constant.

   By definition, $|const(t)| = |\{t\}| = 1 = size(t)$.

2. $t \in \{\mathrm{succ}(t'), \mathrm{pred}(t'), \mathrm{iszero}(t')\}$.

   By IH, $|const(t')| \leq size(t')$.
   By definition and the given result,
   $|const(t)| = |const(t')| \leq size(t') < size(t)$.

Principles of Induction on Terms

Suppose we know for every subterm t' of a term t, $size(t') < size(t)$.

Lemma. For every $t \in \mathcal{T}$, $|const(t)| \leq size(t)$

Proof. By induction on the depth of t. There are three cases to consider.

3. $t =$ if t_1 then t_2 else t_3.

   By IH:

   i. $|const(t_1)| \leq size(t_1)$
   ii. $|const(t_2)| \leq size(t_2)$
   iii. $|const(t_3)| \leq size(t_3)$

$$
\begin{aligned}
|const(t)| &= |const(\text{if } t_1 \text{ then } t_2 \text{ else } t_3)| \\
&= |const(t_1) \cup const(t_2) \cup const(t_3)| \\
&= |const(t_1)| + |const(t_2)| + |const(t_3)| \\
&\leq size(t_1) + size(t_2) + size(t_3) \\
&< size(t)
\end{aligned}
$$

Principles of Induction on Terms

Size gives an induction principle for reasoning about terms:

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

Principles of Induction on Terms

Structural Induction gives an induction principle for reasoning about terms:

If, for each term s,

   given $P(r)$ for all immediate subterms r of s

   we can show $P(s)$,

then $P(s)$ holds for all s.

Principles of Induction on Terms

- Induction on depth or size of terms is analogous to complete induction on natural numbers.
- Ordinary structural induction corresponds to the ordinary natural number induction principle where the induction step requires that $P(n+1)$ be established from just the assumption $P(n)$.
- The choice of one term induction principle over another is determined by which one leads to a simpler structure for the proof at hand.
  - They are inter-derivable.

Principles of Induction on Terms

- Use structural induction wherever possible, since it works on terms directly, avoiding the detour via numbers.
- Most proofs using these principles have a similar structure.

Proof: By induction on $\mathtt{t}$.

Case: $\mathtt{t} = \mathtt{true}$

… show $P(\mathtt{true})$ …

Case: $\mathtt{t} = \mathtt{false}$

… show $P(\mathtt{false})$ …

Case: $\mathtt{t} = \mathtt{if}\ \mathtt{t}_1\ \mathtt{then}\ \mathtt{t}_2\ \mathtt{else}\ \mathtt{t}_3$

… show $P(\mathtt{if}\ \mathtt{t}_1\ \mathtt{then}\ \mathtt{t}_2\ \mathtt{else}\ \mathtt{t}_3)$, using $P(\mathtt{t}_1)$, $P(\mathtt{t}_2)$, and $P(\mathtt{t}_3)$ …

(And similarly for the other syntactic forms.) $\square$