

# Untyped Arithmetic Expressions

Context-free grammar in BNF notation:

$$\begin{aligned} \text{expr} &::= \text{"true"} \mid \text{"false"} \mid \text{"if"} \text{ expr } \text{"then"} \text{ expr } \text{"else"} \text{ expr} \\ &\quad \mid \text{"0"} \mid \text{"succ"} \text{ expr} \mid \text{"pred"} \text{ expr} \mid \text{"iszero"} \text{ expr} \end{aligned}$$
$$\text{value} ::= \text{"true"} \mid \text{"false"} \mid \text{num\_value}$$
$$\text{num\_value} ::= \text{"0"} \mid \text{"succ"} \text{ num\_value}$$

The same context-free grammar in the textbook's notation:

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

# Inductive Definitions

A context-free grammar is an example of an inductively defined set.

## Definition

An **inductively defined set** is the smallest set that obeys a particular set of rules.

## Example

Here's the set of rules for the set *expr*:

- (1)  $true \in expr$
- (2)  $false \in expr$
- (3)  $\forall e_1 e_2 e_3. e_1 \in expr \text{ and } e_2 \in expr \text{ and } e_3 \in expr$   
implies  $(if\ e_1\ then\ e_2\ else\ e_3) \in expr.$
- (4)  $0 \in expr$
- (5)  $\forall e. e \in expr$  implies  $succ\ e \in expr.$
- (6)  $\forall e. e \in expr$  implies  $pred\ e \in expr.$
- (7)  $\forall e. e \in expr$  implies  $iszero\ e \in expr.$

# Horizontal-bar means implication

We often use a horizontal bar to mean implication. Also, we leave implicit the variable quantification (the  $\forall$ s).

## Example

Here's the same set of rules:

$$(1) \frac{}{true \in expr} \quad (2) \frac{}{false \in expr}$$

$$(3) \frac{e_1 \in expr \quad e_2 \in expr \quad e_3 \in expr}{if\ e_1\ then\ e_2\ else\ e_3 \in expr}$$

$$(4) \frac{}{0 \in expr}$$

$$(5) \frac{e \in expr}{succ\ e \in expr}$$

$$(6) \frac{e \in expr}{pred\ e \in expr}$$

$$(7) \frac{e \in expr}{iszero\ e \in expr}$$

# Derivations

The presence of a particular element in an inductively defined set is justified by a tree of rule applications, which is called a **derivation**. We label each rule application with the rule number.

## Example

We know that  $(\text{if } (\text{iszero } 0) \text{ then } 0 \text{ else } (\text{succ } 0)) \in \text{expr}$  because we can build the following derivation:

$$(3) \frac{\begin{array}{ccc} (4) \frac{}{0 \in \text{expr}} & (4) \frac{}{0 \in \text{expr}} & (5) \frac{(4) \frac{}{0 \in \text{expr}}}{\text{succ } 0 \in \text{expr}} \\ (7) \frac{}{\text{iszero } 0 \in \text{expr}} & & \\ \hline \end{array}}{(\text{if } (\text{iszero } 0) \text{ then } 0 \text{ else } (\text{succ } 0)) \in \text{expr}}$$

# Inductive Definitions

Why do we say that an inductively defined set is the *smallest* set that obeys a given set of rules?

Answer: to prevent junk from being allowed in the set.

## Example

"hello world!"  $\notin$  *expr* because there is no derivation that justifies the presence of "hello world!" in the set *expr*.

# Recursive functions

We can define a recursive function on terms by writing a sequence of equations. Here's a function that computes the size of an expression.

$$\begin{aligned} \text{size}(\text{true}) &= 1 \\ \text{size}(\text{false}) &= 1 \\ \text{size}(\text{if } e_1 \text{ then } e_2 \text{ else } e_3) &= 1 + \text{size}(e_1) + \text{size}(e_2) + \text{size}(e_3) \\ \text{size}(0) &= 1 \\ \text{size}(\text{succ } e) &= 1 + \text{size}(e) \\ \text{size}(\text{pred } e) &= 1 + \text{size}(e) \\ \text{size}(\text{iszero } e) &= 1 + \text{size}(e) \end{aligned}$$

# Recursive functions

Here's another function that computes the depth of an expression.

$depth(true)$	$= 1$
$depth(false)$	$= 1$
$depth(\text{if } e_1 \text{ then } e_2 \text{ else } e_3)$	$= 1 + \max(depth(e_1), depth(e_2), depth(e_3))$
$depth(0)$	$= 1$
$depth(succ\ e)$	$= 1 + depth(e)$
$depth(pred\ e)$	$= 1 + depth(e)$
$depth(iszero\ e)$	$= 1 + depth(e)$

We know this function terminates because the recursive calls are applied to arguments that are strictly smaller than the parameter to the recursive function. For example, on line 5 above, the  $e$  in  $depth(e)$  is smaller than the  $succ\ e$  in  $depth(succ\ e)$ .

# Proof by Rule Induction

We can prove properties of inductively defined sets using a special kind of induction called **rule induction**. Suppose we want to prove some property  $P$  about elements of an inductively defined set  $S$ :

$$\forall x. x \in S \text{ implies } P(x)$$

We can prove this by proving something for each rule that defined  $S$ . In particular, for a rule of the form:

$$\frac{b \in S \quad c \in S \quad d \in F}{a \in S}$$

we have to prove that:

$$b \in S \text{ and } c \in S \text{ and } d \in F \text{ and } P(b) \text{ and } P(c) \text{ implies } P(a).$$

(We refer to  $P(b)$  and  $P(c)$  as the **induction hypotheses**.)

# Example Proof by Rule Induction

## Theorem

$\forall e. e \in \text{expr} \text{ implies } \text{depth}(e) \leq \text{size}(e)$

Proof by rule induction on  $e \in \text{expr}$ .

Case  $\boxed{(1) \frac{}{\text{true} \in \text{expr}}}$ : (so  $e = \text{true}$ )

We have  $\text{depth}(\text{true}) = 1$  and  $\text{size}(\text{true}) = 1$  so  $\text{depth}(e) \leq \text{size}(e)$ .

## Example Proof by Rule Induction, continued

Case  $(5) \frac{e' \in \text{expr}}{\text{succ } e' \in \text{expr}}$ : (so  $e = \text{succ } e'$ )

In this case we know that  $e' \in \text{expr}$  and from the induction hypothesis we have  $e' \in \text{expr}$  implies  $\text{depth}(e') \leq \text{size}(e')$ . So we have

$$\begin{aligned} \text{depth}(\text{succ } e') &= 1 + \text{depth}(e') \\ &\leq 1 + \text{size}(e') && \text{by the induction hypothesis} \\ &= \text{size}(\text{succ } e') \end{aligned}$$

Therefore  $\text{depth}(e) \leq \text{size}(e)$ .

## Example Proof by Rule Induction, continued

Case (3)  $\frac{e_1 \in \text{expr} \quad e_2 \in \text{expr} \quad e_3 \in \text{expr}}{\text{if } e_1 \text{ then } e_2 \text{ else } e_3 \in \text{expr}}$  :

(so  $e = \text{if } e_1 \text{ then } e_2 \text{ else } e_3 \in \text{expr}$ )

From the induction hypotheses we have  $\text{depth}(e_1) \leq \text{size}(e_1)$ ,  $\text{depth}(e_2) \leq \text{size}(e_2)$ , and  $\text{depth}(e_3) \leq \text{size}(e_3)$ . Then we have

$$\begin{aligned} \text{depth}(\text{if } e_1 \text{ then } e_2 \text{ else } e_3) &= 1 + \max(\text{depth}(e_1), \text{depth}(e_2), \text{depth}(e_3)) \\ &\leq 1 + \max(\text{size}(e_1), \text{size}(e_2), \text{size}(e_3)) \\ &\leq 1 + \text{size}(e_1) + \text{size}(e_2) + \text{size}(e_3) \\ &= \text{size}(\text{if } e_1 \text{ then } e_2 \text{ else } e_3) \end{aligned}$$

Therefore  $\text{depth}(e) \leq \text{size}(e)$ .

# Inductively Defined Relations

## Definition

A **relation** is a set of tuples.

So everything we've said about sets also applies to relations.

For example, suppose you have an inductively defined relation  $R$  and the following is one of the defining rules for  $R$ :

$$\frac{(a, e, f) \in R \quad e \in S \quad f \in T}{(a, b, c) \in R}$$

Suppose you want to prove:

$\forall x, y, z. (x, y, z) \in R \text{ implies } P(x, y, z)$ . Then for the above rule, you'd need to prove:

$(a, e, f) \in R$  and  $e \in S$  and  $f \in T$  and  $P(a, e, f)$   
implies  $P(a, b, c)$ .