Inductive Definitions with Inference Rules

Outline

Introduction

Specifying inductive definitions
- Inference rules in action
- Judgments, axioms, and rules

Reasoning about inductive definitions
- Direct proofs
- Admissibility
- Rule induction

What are inference rules?

Inference rules – a mathematical metalanguage

For **specifying** and **formally reasoning** about **inductive definitions**

Inductive definition

Recursively defines something in terms of itself

premises

$$\frac{Human(x) \rightarrow Mortal(x) \qquad Human(x)}{Mortal(x)}$$

conclusion

Outline

Other metalanguages for inductive definitions

Haskell data types

```
data Nat = Z | S Nat
data Exp = Add Exp Exp
         | Neg Exp
         | Lit Nat
```

Recursive functions in Haskell

```
even :: Nat -> Bool
even Z         = True
even (S Z)     = False
even (S (S n)) = even n
```

Grammars

$$
\begin{array}{rcl}
n \in \mathit{Nat} & ::= & \mathtt{Z} \mid \mathtt{S}\ n \\
e \in \mathit{Exp} & ::= & \mathtt{add}\ e\ e \\
& \mid & \mathtt{neg}\ e \\
& \mid & n
\end{array}
$$

Can also define all of these with **inference rules**!

Example: defining syntax by inference rules

Grammars

$$
\begin{array}{rcl}
n \in \mathit{Nat} & ::= & \mathbf{Z} \mid \mathbf{S}\ n \\
e \in \mathit{Exp} & ::= & \mathbf{add}\ e\ e \\
& \mid & \mathbf{neg}\ e \\
& \mid & n
\end{array}
$$

rule schema

$$\mathbf{Z} \in \mathit{Nat} \qquad \frac{n \in \mathit{Nat}}{\mathbf{S}\ n \in \mathit{Nat}}$$

axiom
(no premises)

$$\frac{n \in \mathit{Nat}}{n \in \mathit{Exp}} \qquad \frac{e \in \mathit{Exp}}{\mathbf{neg}\ e \in \mathit{Exp}}$$

$$\frac{e_1 \in \mathit{Exp} \qquad e_2 \in \mathit{Exp}}{\mathbf{add}\ e_1\ e_2 \in \mathit{Exp}}$$

Example: defining a predicate

Recursive function in Haskell

```
even :: Nat -> Bool
even Z          = True
even (S Z)      = False
even (S (S n)) = even n
```

Option 1: Constructive judgment

$$\mathit{Even}(\mathbf{Z}) \qquad \frac{\mathit{Even}(n)}{\mathit{Even}(\mathbf{S}\ \mathbf{(S}\ n\mathbf{)})}$$

Option 2: Relate inputs to outputs

$$\mathit{Even}(\mathbf{Z}, \mathbf{true}) \qquad \mathit{Even}(\mathbf{S}\ \mathbf{Z}, \mathbf{false})$$

$$\frac{\mathit{Even}(n, b)}{\mathit{Even}(\mathbf{S}\ \mathbf{(S}\ n\mathbf{)}, b)}$$

Outline

The structure of a definition

How to define a "concept" in three parts:

1. **syntax** – how to express the concept
2. **type** – what kind of information is it?
3. **content** – the definition itself

Example: dictionary definition

Syntax:	e·ven |ˈēvən|
Type:	adjective
Content:	(of a number) divisible by two without a remainder

Example: function definition

```
even :: Nat -> Bool
even Z           = True
even (S Z)       = False
even (S (S n))   = even n
```

How to define a concept using inference rules

1. Define a **judgment form** – syntax and type

States that one or more values have some **property**
or exist in some **relation** to each other

2. Write down the **rules** for the judgment – content

- **axioms** – base cases, only conclusion
- **proper rules** – recursive cases, premises + conclusion

Judgments

1. Define a judgment form – syntax and type

States that one or more values have some **property** or exist in some **relation** to each other

Syntax	Type	Property or relation
$n \in Nat$	AST	n is in the syntactic category Nat
$Even(n)$	Nat	n is an even number
$n_1 < n_2$	$Nat \times Nat$	n_1 is less than n_2
$e : T$	$Exp \times Type$	e has type T
$\Gamma \vdash e : T$	$Env \times Exp \times Type$	e has type T in environment Γ

Set theoretic view of judgments

A judgment is (conceptually) a **predicate** that indicates set membership

Example: $Even(n) \subseteq Nat$

$$
\begin{aligned}
Even &: Nat \to \mathbb{B} \\
&= \{(\mathtt{Z}, true),\ (\mathtt{S\,Z}, false),\ (\mathtt{S\,(S\,Z)}, true),\ \ldots\} \\
&\equiv \{\mathtt{Z},\ \mathtt{S\,(S\,Z)},\ \mathtt{S\,(S\,(S\,(S\,Z)))},\ \ldots\} \subseteq Nat
\end{aligned}
$$

Example: $n_1 < n_2 \subseteq Nat \times Nat$

$$
\begin{aligned}
< &: Nat \times Nat \to \mathbb{B} \\
&= \{((\mathtt{0},\mathtt{0}), false),\ ((\mathtt{0},\mathtt{1}), true),\ \ldots\ ((\mathtt{5},\mathtt{3}), false),\ \ldots\ ((\mathtt{5},\mathtt{7}), true),\ \ldots\} \\
&\equiv \{(\mathtt{0},\mathtt{1}),\ \ldots\ (\mathtt{5},\mathtt{7}), \ldots\} \subseteq Nat \times Nat
\end{aligned}
$$

Giving meaning to a judgment by inference rules

2. Write down the rules of the judgment – content

- **axioms** – base cases, only conclusion
- **proper rules** – recursive cases, premises + conclusion

Inductively defines the **instances** of a judgment (i.e. members of its set)

Rules for: $Even(n) \subseteq Nat$

$$Even(\mathbf{Z}) \qquad \frac{Even(n)}{Even(\mathbf{S}\ (\mathbf{S}\ n))}$$

Rules for: $n_1 < n_2 \subseteq Nat \times Nat$

$$\mathbf{Z} < \mathbf{S}\ \mathbf{Z} \qquad \frac{n_1 < n_2}{n_1 < \mathbf{S}\ n_2} \qquad \frac{n_1 < n_2}{\mathbf{S}\ n_1 < \mathbf{S}\ n_2}$$

Exercises

1. Define the judgment: $Odd(n) \subseteq Nat$

2. Define the judgment: $n_1 + n_2 = n_3 \subseteq Nat \times Nat \times Nat$

For reference:

Rules for: $Even(n) \subseteq Nat$

$$Even(\mathbf{Z}) \qquad \frac{Even(n)}{Even(\mathbf{S}\ \mathbf{(}\mathbf{S}\ n\mathbf{)})}$$

Rules for: $n_1 < n_2 \subseteq Nat \times Nat$

$$\mathbf{Z} < \mathbf{S}\ \mathbf{Z} \qquad \frac{n_1 < n_2}{n_1 < \mathbf{S}\ n_2} \qquad \frac{n_1 < n_2}{\mathbf{S}\ n_1 < \mathbf{S}\ n_2}$$

Outline

Expressing claims

We can also use inference rules to express **claims** about judgments

Examples

$$\mathbf{S}\ (\mathbf{S}\ \mathbf{Z}) \in \mathit{Nat} \qquad \frac{\mathit{Even}(\mathbf{S}\ n)}{\mathit{Odd}(n)} \qquad \frac{n_1 < n_2 \qquad n_2 < n_3}{n_1 < n_3} \qquad \frac{n_1 + n_2 = n_3}{n_2 + n_1 = n_3}$$

How can we **prove** these claims?

Three main techniques:

1. **direct proof** – derive conclusion from premises using the definition
2. **admissibility** – derive conclusion from derivations of premises
3. **rule induction** – reason inductively using the definition

Outline

Direct proof by derivation

Definition: $n \in Nat$

$$\mathbf{Z} \in Nat \qquad \text{Succ}\ \frac{n \in Nat}{\mathbf{S}\ n \in Nat}$$

$$\text{Succ}\ \dfrac{\text{Succ}\ \dfrac{\mathbf{Z} \in Nat}{\mathbf{S}\,\mathbf{Z} \in Nat}}{\mathbf{S}\,(\mathbf{S}\,\mathbf{Z}) \in Nat}$$

Definition: $n_1 < n_2 \subseteq Nat \times Nat$

$$\mathbf{Z} < \mathbf{S}\,\mathbf{Z} \qquad \text{S}\ \frac{n_1 < n_2}{n_1 < \mathbf{S}\ n_2} \qquad \text{+1}\ \frac{n_1 < n_2}{\mathbf{S}\ n_1 < \mathbf{S}\ n_2}$$

$$\text{+1}\ \dfrac{\text{S}\ \dfrac{\mathbf{Z} < \mathbf{S}\,\mathbf{Z}}{\mathbf{Z} < \mathbf{S}\,(\mathbf{S}\,\mathbf{Z})}}{\mathbf{S}\,\mathbf{Z} < \mathbf{S}\,(\mathbf{S}\,(\mathbf{S}\,\mathbf{Z}))}$$

Proof trees

Definition: $e \in Exp$

Axioms: $\mathtt{0} \in Nat,\ \mathtt{1} \in Nat,\ \mathtt{2} \in Nat,\ \ldots$

$$\text{lit}\ \frac{n \in Nat}{n \in Exp} \qquad \text{neg}\ \frac{e \in Exp}{\mathbf{neg}\ e \in Exp} \qquad \text{add}\ \frac{e_1 \in Exp \qquad e_2 \in Exp}{\mathbf{add}\ e_1\ e_2 \in Exp}$$

$$\text{add}\ \frac{\text{add}\ \dfrac{\text{lit}\ \dfrac{\mathtt{2} \in Nat}{\mathtt{2} \in Exp} \qquad \text{lit}\ \dfrac{\mathtt{3} \in Nat}{\mathtt{3} \in Exp}}{\mathtt{add\ 2\ 3} \in Exp} \qquad \text{neg}\ \dfrac{\text{lit}\ \dfrac{\mathtt{4} \in Nat}{\mathtt{4} \in Exp}}{\mathtt{neg\ 4} \in Exp}}{\mathtt{add\ (add\ 2\ 3)\ (neg\ 4)} \in Exp}$$

Exercises

Prove that the following expressions are valid terms in Exp

1. `neg (add 5 (neg 2))`
2. `add (neg (neg 3)) 4`

Definition: $e \in Exp$

Axioms: $\mathbf{0} \in Nat,\ \mathbf{1} \in Nat,\ \mathbf{2} \in Nat,\ \ldots$

$$\text{lit}\ \frac{n \in Nat}{n \in Exp} \qquad \text{neg}\ \frac{e \in Exp}{\textbf{neg}\ e \in Exp} \qquad \text{add}\ \frac{e_1 \in Exp \qquad e_2 \in Exp}{\textbf{add}\ e_1\ e_2 \in Exp}$$

Outline

Admissibility

Construct proofs from assumed **derivations of the premises**

Insights:

- If the premise of a claim is satisfied, it must have a derivation
- Can use information in the derivations to prove the conclusion

Proof technique

Show that **all possible derivations** of premises yield a proof of the conclusion

Apply definition rules backwards on the premises, prove for each case!

Super simple example

Definition: $n \in Nat \subseteq AST$

$$\mathbf{Z} \in Nat \qquad \text{Succ}\ \frac{n \in Nat}{\mathbf{S}\ n \in Nat}$$

Bold claim

$$\frac{\mathbf{S}\ (\mathbf{S}\ n) \in Nat}{n \in Nat}$$

Proof sketch:

- Enumerate derivations of premise
- Show that each derivation proves the conclusion

Only possible derivation

$$\text{Succ}\ \frac{\text{Succ}\ \dfrac{\boxed{n \in Nat}}{\mathbf{S}\ n \in Nat}}{\mathbf{S}\ (\mathbf{S}\ n) \in Nat}$$

Outline

Rule induction

Just like structural induction on inductive data types!

Definition: $e \in Exp \subseteq AST$

$$\frac{n \in Nat}{n \in Exp} \qquad \frac{e \in Exp}{\textbf{neg}\ e \in Exp} \qquad \frac{e_1 \in Exp \qquad e_2 \in Exp}{\textbf{add}\ e_1\ e_2 \in Exp}$$

Suppose I want to prove property P on all Exps. Just prove:

- $\forall n \in Nat, P(n)$
- $P(e) \to P(\textbf{neg}\ e)$
- $P(e_1) \to P(e_2) \to P(\textbf{add}\ e_1\ e_2)$