Inductive Definitions with Inference Rules

Introduction

Specifying inductive definitions

Inference rules in action Judgments, axioms, and rules

Reasoning about inductive definitions

Direct proofs

Admissibility

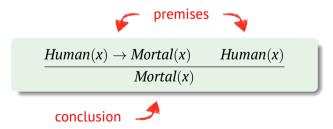
What are inference rules?

Inference rules – a mathematical metalanguage

For specifying and formally reasoning about inductive definitions

Inductive definition

Recursively defines something in terms of itself



Introduction 3/25

Introduction

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

Reasoning about inductive definitions

Direct proofs

Admissibility

Rule induction

Specifying inductive definitions 4/25

Other metalanguages for inductive definitions

Haskell data types

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

Grammars

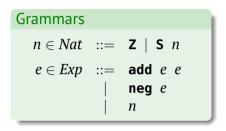
Recursive functions in Haskell

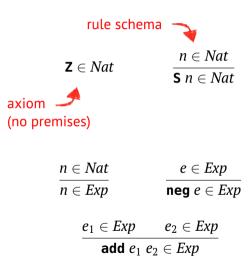
```
even :: Nat -> Bool
even Z = True
even (S Z) = False
even (S (S n)) = even n
```

Can also define all of these with inference rules!

Specifying inductive definitions 5 / 25

Example: defining syntax by inference rules





Specifying inductive definitions 6 / 25

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

Even(**Z**)
$$\frac{Even(n)}{Even(S (S n))}$$

Option 2: Relate inputs to outputs

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

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

Specifying inductive definitions 7 / 25

Introduction

Specifying inductive definitions

Inference rules in action Judgments, axioms, and rules

Reasoning about inductive definitions

Direct proofs
Admissibility
Rule induction

Specifying inductive definitions 8 / 25

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 |'ēvən|

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
```

Specifying inductive definitions 9/25

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

Specifying inductive definitions 10 / 25

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

Specifying inductive definitions 11/25

Set theoretic view of judgments

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

```
Example: Even(n) \subseteq Nat

Even : Nat \to \mathbb{B}

= \{ (\mathbf{Z}, true), (\mathbf{SZ}, false), (\mathbf{SSZ}), true), \ldots \}

\equiv \{ \mathbf{Z}, \mathbf{SSZ}), \mathbf{SSSS}), \ldots \} \subseteq Nat
```

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

<: Nat \times Nat \rightarrow \mathbb{B}

= \{((\mathbf{0}, \mathbf{0}), false), ((\mathbf{0}, \mathbf{1}), true), \dots ((\mathbf{5}, \mathbf{3}), false), \dots ((\mathbf{5}, \mathbf{7}), true), \dots\}

\equiv \{(\mathbf{0}, \mathbf{1}), \dots (\mathbf{5}, \mathbf{7}), \dots\} \subseteq Nat \times Nat
```

Specifying inductive definitions 12/25

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

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

Specifying inductive definitions 13/25

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

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

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

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

Specifying inductive definitions 14/25

Introduction

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

Reasoning about inductive definitions

Direct proofs

Admissibility

Expressing claims

We can also use inference rules to express claims about judgments

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

Introduction

Specifying inductive definitions

Inference rules in action Judgments, axioms, and rules

Reasoning about inductive definitions

Direct proofs

Admissibility

Pula industic

Direct proof by derivation

Definition: $n \in Nat$

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

Succ
$$\frac{\mathbf{Z} \in Nat}{\mathbf{S} \mathbf{Z} \in Nat}$$

Succ $\frac{\mathbf{S} \mathbf{S} \in Nat}{\mathbf{S} (\mathbf{S} \mathbf{Z}) \in Nat}$

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

$${f Z} < {f S} \ {f Z}$$
 ${f S} \ rac{n_1 < n_2}{n_1 < {f S} \ n_2}$ +1 $rac{n_1 < n_2}{{f S} \ n_1 < {f S} \ n_2}$

$$+1 \ rac{{\sf Z} < {\sf S} \, {\sf Z}}{{\sf Z} < {\sf S} \, ({\sf S} \, {\sf Z})}$$

Proof trees

Definition: $e \in Exp$ Axioms: $\mathbf{0} \in Nat$, $\mathbf{1} \in Nat$, $\mathbf{2} \in Nat$, ... lit $\frac{n \in Nat}{n \in Exp}$ neg $\frac{e \in Exp}{\mathsf{neg}\ e \in Exp}$ add $\frac{e_1 \in Exp}{\mathsf{add}\ e_1\ e_2 \in Exp}$

$$\begin{array}{c} \text{lit} \\ \text{add} \\ \text{add} \\ \text{add} \\ \hline \\ \text{add} \\ \text{add} \\ \hline \\ \text{add} \\ \text{add} \\ \textbf{(add 2 3)} \\ \end{array} \quad \begin{array}{c} \text{lit} \\ \frac{\textbf{4} \in Nat}{\textbf{4} \in Exp} \\ \text{neg} \\ \hline \\ \text{neg 4} \in Exp \\ \hline \\ \text{add (add 2 3)} \\ \end{array}$$

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, ...

lit \frac{n \in Nat}{n \in Exp} neg \frac{e \in Exp}{\mathsf{neg}\ e \in Exp} add \frac{e_1 \in Exp}{\mathsf{add}\ e_1\ e_2 \in Exp}
```

Introduction

Specifying inductive definitions

Inference rules in action Judgments, axioms, and rules

Reasoning about inductive definitions

Direct proofs

Admissibility

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

Introduction

Specifying inductive definitions

Judgments, axioms, and rules

Reasoning about inductive definitions

Direct proofs

Admissibility

Rule induction

Just like structural induction on inductive data types!

$$\begin{array}{ccc} \text{Definition:} & e \in Exp & \subseteq AST \\ \\ \frac{n \in Nat}{n \in Exp} & \frac{e \in Exp}{\mathsf{neg} \ e \in Exp} & \frac{e_1 \in Exp}{\mathsf{add} \ e_1 \ e_2 \in Exp} \end{array}$$

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

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