15-312 Lecture on Inductive Proofs

Proving Properties of Judgments

- Typical format of a statement about judgments:

  > *For every derivation $\mathcal{D}$ of judgment J, there exists derivation $\mathcal{D}'$ of judgment J'*

  We will abbreviate it as

  > *For every $\mathcal{D} :: J$, there exists $\mathcal{D}' :: J'$*

- Proof proceeds by induction on the construction of the given derivation $\mathcal{D}$.
  - Called *rule induction, structural induction, induction on the structure of derivations, . . .*
  - One case for each rule defining J (generally all rules, but sometimes only a subset can have been applied)
  - Induction hypothesis assumes that the property holds of the premises of each rule.
  - Use IH and rules to build derivations $\mathcal{D}'$
  - Possible because deductive systems are assumed to be closed

Example

In the deductive system

$$\frac{}{\mathsf{z}\ \mathsf{nat}}\ \mathbf{z\_nat} \qquad\qquad \frac{n\ \mathsf{nat}}{\mathsf{s}\ n\ \mathsf{nat}}\ \mathbf{s\_nat}$$

Prove that if a nat, *then* $a = \mathsf{z}$, *or* $a = \mathsf{s}\ \mathsf{z}$, *or* $a = \mathsf{s}(\mathsf{s}\ b)$ *for* b nat

Let's rephrase it more formally:

Property 1 *For every derivation $\mathcal{D} :: a$ nat, either $a = \mathsf{z}$, or $a = \mathsf{s}\ \mathsf{z}$, or $a = \mathsf{s}(\mathsf{s}\ b)$ and there exists a derivation $\mathcal{E} :: b$ nat.*

Proof: By induction on the structure of $\mathcal{D}$. Because there are two rules defining the judgment $a \;\; nat$, there are two inductive cases to examine:

1. Case

$$\mathcal{D} = \frac{}{\mathsf{z}\ \mathsf{nat}}\ \mathbf{z\_nat}$$

   Then, it must be the case that $a = \mathsf{z}$, which is one of the possible conclusions of this property.

2. Case

$$\mathcal{D} = \frac{\begin{array}{c}\mathcal{D}' \\ n\ \mathsf{nat}\end{array}}{\mathsf{s}\, n\ \mathsf{nat}}\ \mathbf{s\_nat}$$

   Then it must be the case that $a = \mathsf{s}\, n$ and we know that $\mathcal{D}'$ is a derivation of n nat.

   The induction hypothesis allows us to conclude that either $n = \mathsf{z}$, or $n = \mathsf{s}\,\mathsf{z}$, or $n = \mathsf{s}(\mathsf{s}\, n')$ such that there is a derivation $\mathcal{E}'$ of n' nat. We need to examine each of these possibilities as a subcase of the proof.

   (a) Subcase $n = \mathsf{z}$: then $a = \mathsf{s}\,\mathsf{z}$, which is one of the possible conclusions of this property.

   (b) Subcase $n = \mathsf{s}\,\mathsf{z}$: then $a = \mathsf{s}(\mathsf{s}\,\mathsf{z})$. This allows us to take b to be z, but we must construct a derivation $\mathcal{E}$ of z nat. To do this, we simply use rule $\mathbf{z\_nat}$:

$$\mathcal{E} = \frac{}{\mathsf{z}\ \mathsf{nat}}\ \mathbf{z\_nat}$$

   (c) Subcase $n = \mathsf{s}(\mathsf{s}\, n')$ and there is a derivation $\mathcal{E}'$ of n' nat. Then $a = \mathsf{s}(\mathsf{s}(\mathsf{s}\, n'))$ and we can take b to be $\mathsf{s}\, n'$. To construct the required derivation $\mathcal{E}$ of $\mathsf{s}\, n'$, we simply take $\mathcal{E}'$ and extend it by applying rule $\mathbf{s\_nat}$:

$$\mathcal{E} = \frac{\begin{array}{c}\mathcal{E}' \\ n'\ \mathsf{nat}\end{array}}{\mathsf{s}\, n'\ \mathsf{nat}}\ \mathbf{s\_nat}$$

   Having obtained the desired conclusion for each subcase, we have completed the proof of the case in which $\mathcal{D}$ ended with rule $\mathbf{s\_nat}$.

Having obtained the desired conclusion for every possible rule that could appear at the end of $\mathcal{D}$, we have proved the property. □

Iterated and Simultaneous Judgments

- Deductive systems can (and often do) define several judgments
- Simultaneous definition if rules depend on each other
- Iterated definitions if rule dependency flows one way only
- Proof technique remains the same (but need evidence for dependent judgments)
  - For simultaneous judgments, often simultaneous statement for each judgment form

Derivable and Admissible Rules

Rules that are consequences of the rules already present in a deductive system

Derivable Rules

- Shortcuts
- Obtained as a schematic derivation snippet. E.g.,

$$\frac{n\ \mathsf{nat}}{\mathsf{s}(\mathsf{s}\ n)\ \mathsf{nat}}\ \mathbf{ss\_nat} \qquad \text{is derivable since it is a shortcut for} \qquad \frac{\dfrac{n\ \mathsf{nat}}{\mathsf{s}\ n\ \mathsf{nat}}\ \mathbf{s\_nat}}{\mathsf{s}(\mathsf{s}\ n)\ \mathsf{nat}}\ \mathbf{s\_nat}$$

- Remain derivable if rule set is extended

Admissible Rules

- Cannot be expressed as shortcuts
- Verified by doing an inductive proof. E.g.,

$$\frac{\mathsf{s}\ n\ \mathsf{nat}}{n\ \mathsf{nat}}\ \mathbf{nat\_s}$$

  checked to be admissible by proving that

  For every derivation $\mathcal{D} :: \mathsf{s}\ n\ \mathsf{nat}$*, there is a derivation* $\mathcal{D}' :: n\ \mathsf{nat}$.

- Rule may not be admissible in an extended rule set. E.g., with the addition of

$$\frac{}{\mathsf{s}\ \clubsuit\ \mathsf{nat}}\ \mathbf{s\clubsuit\_nat}$$

  rule $\mathbf{nat\_s}$ no more admissible (but rule $\mathbf{ss\_nat}$ remains derivable)

Exercises

- In a deductive system containing the rules for $\_$ nat and $\mathsf{sum}(\_,\_,\_)$ — see Harper's book, prove that:

  If $\mathcal{D} :: \mathsf{sum}(m, n, p)$*, then there exists derivations* $\mathcal{D}_m :: m$ nat*,* $\mathcal{D}_n :: n$ nat *and* $\mathcal{D}_p :: p$ nat*,*

- In the standard deductive system for transition sequences (see Harper's book, Sec. 4.1 and 4.2), show that the following rule is admissible:

  $$\frac{s \mapsto^* s' \quad s' \mapsto s''}{s \mapsto^* s''}$$

  Is it derivable?