Harvard School of Engineering and Applied Sciences — CS 152: Programming Languages

Proving the Induction Principle

Spring 2017

The induction principle for natural numbers is usually a theorem, a consequence of other properties of natural numbers taken as primitive. For instance, the following:

Well-Ordering Axiom. *Every nonempty subset of* $\mathbb{N}$ *contains a smallest element.*

(You need an axiom like the Well-Ordering Axiom as part of what it means to take natural numbers as primitives. If you derive the natural numbers in a set theory like ZF, then you can derive the Well-Ordering Axiom from a corresponding principle in ZF such as the Foundation Axiom.)

Theorem 1 (Induction Principle for Natural Numbers)**.** *Let* $P(n)$ *be a property of natural numbers. If*

(i) $P(0)$ *holds;*

(ii) for all $k \in \mathbb{N}$*, if* $P(k)$ *holds then* $P(k+1)$ *holds;*

then for all $n \in \mathbb{N}$*,* $P(n)$ *holds.*

Proof. Let P be a property of the natural numbers for which (i) and (ii) are both true. Let S be the set of all $j \in \mathbb{N}$ such that $P(j)$ does *not* hold. It suffices to show that S is empty for the result to follow.

Let's argue by contradiction. Suppose that S is not empty. Then by the Well-Ordering Axiom, there is a least element $d \in S$. Since $d \in S$, then $P(d)$ is false. Since $P(0)$ is true by (i), $d \neq 0$, and thus $d \geq 1$. Since $d \geq 1$, then $d-1 \in \mathbb{N}$. Moreover, $P(d-1) \notin S$, because $d-1 < d$ and d was the least element of S. Since $P(d-1) \notin S$, $P(d-1)$ is true. But property (ii) tells us that if $P(d-1)$ is true, then $P(d)$ must be true as well, contradicting the fact that we have $P(d)$ false. Since we derive a contradiction, our initial assumption that S is not empty must be false, that is, S is empty. $\square$

In a similar way, the induction principle for an arbitrary inductively-defined set is a theorem that we can prove. In fact, can prove the induction principle for an inductively-defined set using the induction principle for natural numbers! Basically, we proceed by induction on the height of proof trees defining membership in the inductively-defined set.

Theorem 2 (Induction Principle for Inductively-Defined Sets)**.** *Let* A *be an inductively-defined set, given by axioms* $\mathcal{A}$ *and inference rules* $\mathcal{I}$*. Let* P *be a propery of elements of* A*. If:*

(i) for every axiom in $\mathcal{A}$ *of the form* $\dfrac{}{a \in A}$ *,* $P(a)$ *holds;*

(ii) for every inference rule in $\mathcal{I}$ *of the form* $\dfrac{a_1 \in A \ldots a_k \in A}{a \in A}$ *, if* $P(a_1), \ldots, P(a_k)$ *hold then* $P(a)$ *holds;*

then for all $a \in A$*,* $P(a)$ *holds.*

Proof. Let A be an inductively-defined set given by axioms $\mathcal{A}$ and inference rules $\mathcal{I}$. Let $P(a)$ be a property of elements of A for which (i) and (ii) are both true.

We want to show that for all $a \in A$, $P(a)$ holds. Since $a \in A$ exactly when there is a finite proof tree showing $a \in A$ according to $\mathcal{A}$ and $\mathcal{I}$, it suffices to show that for all $n \in \mathbb{N}$ and for all $a \in A$ with a proof tree of height at most $n+1$, $P(a)$ holds. (Proof trees must have height at least 1.) This is the kind of property we can prove by induction on the natural numbers. Here is the property we actually prove, by induction on n:

$$P'(n) = \forall a \in A \text{ with a proof tree of height at most } n+1,\ P(a) \text{ holds}$$

- **Case $n = 0$:** If $a \in A$ with a proof tree of height at most 1, then $a \in A$ must be given by some axiom $\dfrac{}{a \in A}$. By (i), this means that $P(a)$ holds, as required.
- **Case $n = k + 1$:** If $a \in A$ with a proof tree of height at most $k + 1$, then either the proof tree has height 1, or has height greater than 1.
  - If the proof tree has height 1, then $a \in A$ must be given by some axiom $\dfrac{}{a \in A}$. By (i), this means that $P(a)$ holds, as required.
  - If the proof tree has height greater than 1, then the rule of the proof tree with conclusion $a \in A$ must be an inference rule in $\mathcal{I}$ of the form $\dfrac{a_1 \in A \ldots a_k \in A}{a \in A}$. That we have a proof tree for $a \in A$ means that we have a proof tree for each premise $a_i \in A$, and each such proof tree has height at most k. By the induction hypothesis, we therefore know that $P(a_1), \ldots, P(a_k)$ hold. By property (ii), this means that $P(a)$ holds, as required.

Therefore, for all $n \in \mathbb{N}$, $P'(n)$ holds; that is, for all $a \in A$, $P(a)$ holds. □