Induction

Alex Kavvos

Reading: PFPL, §2.4, 2.5, 2.6, 3.1

Recall the rules that generate the natural numbers:

$$\frac{}{\mathsf{zero}\ \mathsf{nat}}\ \textsc{Zero} \qquad\qquad \frac{n\ \mathsf{nat}}{\mathsf{succ}(n)\ \mathsf{nat}}\ \textsc{Succ}$$

These rules define all the ways of constructing a natural number. Thus, if we *prove* that the truth of a property is preserved by these two rules, it must be that we have proved it for all natural numbers.

This is called the *principle of induction.*

Stated for the natural numbers, the principle of induction is as follows:

> Let $\mathcal{P}$ be a property of the natural numbers. If
>
> - $\mathcal{P}(\mathsf{zero})$, and
> - whenever $\mathcal{P}(n)$ we know that $\mathcal{P}(\mathsf{succ}(n))$
>
> then $\mathcal{P}(n)$ for all n nat.

Every set of rules generates an associated induction principle. Thus, the usual principle of natural number induction is implicitly generated by the rules Zero and Succ.

We can use induction to prove results.

Claim 1. If $\mathsf{succ}(n)$ nat then n nat.

To prove this it suffices to prove the following property by induction.

> $\mathcal{P}(n)$: "If n nat and $n = \mathsf{succ}(x)$ for some x, then x nat."

1 Derivable and admissible rules

Statements like Claim 1 are often written as rules themselves: $\dfrac{\mathsf{succ}(n)\ \mathsf{nat}}{n\ \mathsf{nat}}$

This rule is not one of the defining rules of natural numbers. Rather, it is an admissible rule.

A rule is **admissible** if whenever we have a derivation of the premises, then we know we can construct a derivation of the conclusion.

In this particular instance, given a derivation of $\mathsf{succ}(n)$ nat, we can construct a derivation of n nat by trimming the last line of the derivation. For $n \stackrel{\text{def}}{=} \mathsf{succ}(\mathsf{zero})$:

$$\dfrac{\dfrac{\dfrac{}{\mathsf{zero}\ \mathsf{nat}}}{\mathsf{succ}(\mathsf{zero})\ \mathsf{nat}}}{\mathsf{succ}(\mathsf{succ}(\mathsf{zero}))\ \mathsf{nat}} \quad\rightsquigarrow\quad \dfrac{\dfrac{}{\mathsf{zero}\ \mathsf{nat}}}{\mathsf{succ}(\mathsf{zero})\ \mathsf{nat}}$$

This is what the proof of Claim 1 implicitly does.

Admissible rules imply some non-trivial reasoning. When there is no such requirement, a rule is called derivable.

A rule is **derivable** if we can use a derivation of its premise as a building block in deriving its conclusion.

For example, the following rule is derivable: $\dfrac{n\ \mathsf{nat}}{\mathsf{succ}(\mathsf{succ}(n))\ \mathsf{nat}}$

Indeed, if we have a derivation of the premise, all it takes is two uses of the rule Succ:

$$\dfrac{\vdots}{n\ \mathsf{nat}} \quad \rightsquigarrow \quad \dfrac{\dfrac{\dfrac{\vdots}{n\ \mathsf{nat}}}{\mathsf{succ}(n)\ \mathsf{nat}}\ \textsc{Succ}}{\mathsf{succ}(\mathsf{succ}(n))\ \mathsf{nat}}\ \textsc{Succ}$$

There is no need to perform induction to show that a rule is derivable.

2 Simultaneous induction

The principle of induction also applies to the simultaneous generation of judgements in a natural way. Recall the mutually inductive generation of the judgments n even and n odd by the rules

$$\overset{\textsc{EvenZ}}{\dfrac{}{\mathsf{zero\ even}}} \qquad \overset{\textsc{Odd}}{\dfrac{n\ \mathsf{even}}{\mathsf{succ}(n)\ \mathsf{odd}}} \qquad \overset{\textsc{Even}}{\dfrac{n\ \mathsf{odd}}{\mathsf{succ}(n)\ \mathsf{even}}}$$

The associated induction principle is as follows:

> Let $\mathcal{P}$ be a property of even numbers, and let $\mathcal{Q}$ be a property of odd numbers. If
>
> - $\mathcal{P}(\mathsf{zero})$, and
> - whenever n even and $\mathcal{P}(n)$ we have $\mathcal{Q}(\mathsf{succ}(n))$, and
> - whenever n odd and $\mathcal{Q}(n)$ we have $\mathcal{P}(\mathsf{succ}(n))$,
>
> then $\mathcal{P}(n)$ for all n even, and $\mathcal{Q}(n)$ for all n odd.

For example, we can prove that

Claim 2. If n even then either $n = \mathsf{zero}$ or $n = \mathsf{succ}(x)$ where x odd.

We cannot prove this by a simple induction; we need to **strengthen** the inductive hypothesis. The proof amounts to performing simultaneous induction over the following predicates $\mathcal{P}$ and $\mathcal{Q}$.

> $\mathcal{P}(n)$: "If n even then either $n = \mathsf{zero}$ or $n = \mathsf{succ}(x)$ where x odd."
>
> $\mathcal{Q}(n)$: "If n odd then $n = \mathsf{succ}(x)$ where x even."

The claim itself amounts to $\mathcal{P}(n)$ for all n even.