Last time we talked about structural induction and how it is a generalization of classic mathematical induction. Today we will discuss an even more general form of induction: *well-founded induction*. This principle will help to illuminate why all forms induction are mathematically valid.

1 Free Variables Revisited

We talked last time about the definition of free variables for ARITH:

$$\begin{aligned}
\mathrm{FV}(n) &= \emptyset \\
\mathrm{FV}(x) &= \{x\} \\
\mathrm{FV}(e_1 + e_2) &= \mathrm{FV}(e_1) \cup \mathrm{FV}(e_2) \\
\mathrm{FV}(e_1 * e_2) &= \mathrm{FV}(e_1) \cup \mathrm{FV}(e_2) \\
\mathrm{FV}(x := e_1 \,;\, e_2) &= \mathrm{FV}(e_1) \cup (\mathrm{FV}(e_2) - \{x\})
\end{aligned}$$

Why does this definition uniquely determine the function FV? If we think of it as an inductively defined relation $\mathrm{FV} \subseteq \mathbf{Exp} \times 2^{\mathbf{Var}}$, there are two issues.

- *Uniqueness*: Is there (at most) one $V \subseteq \mathbf{Var}$ such that $(e, V) \in \mathrm{FV}$ for all $e \in \mathbf{Exp}$? That is, is FV a function?
- *Existence*: Is FV defined on all ARITH terms? In other words, is it total?

We discussed last time how this was a structurally-inductive (or structurally-recursive) definition. There are exactly five clauses of the FV, one for each clause in the BNF definition of ARITH syntax, and that expressions can be formed only in these five ways. Critically, although FV appears on the right side of three of the five clauses, in each case it is applied to a proper (*proper* = strictly) subterm. Intuitively, this last point means that the term it is applied to is always shrinking, and FV will eventually "bottom out" at one of the first two clauses. Now let's make that intuition precise.

2 Well-Founded Relations

Definition 1. A binary relation $\prec$ is said to be *well-founded* if it has no infinite descending chains.
An *infinite descending chain* is an infinite sequence $a_0, a_1, a_2, \ldots$ such that $a_{i+1} \prec a_i$ for all $i \geq 0$.

Note that a well-founded relation cannot be reflexive, as an infinite stream of the same value would then be an infinite descending chain.

Here are some examples of well-founded relations.

- The successor relation $\{(m, m+1) \mid m \in \mathbb{N}\}$ on the natural numbers $\mathbb{N}$.
- The (strict) less-than relation $<$ on $\mathbb{N}$.
- The (strict) sub-expression relation on ARITH expressions.
- The element-of relation $\in$ on sets. The axiom of foundation (or axiom of regularity) in Zermelo–Fraenkel (ZF) set theory implies that $\in$ is well-founded. Among other things, it prevents a set from containing itself.
- The proper subset relation $\subset$ on *finite* subsets of $\mathbb{N}$.

The following are *not* well-founded relations.

- The predecessor relation $\{(m+1, m) \mid m \in \mathbb{N}\}$ on the natural numbers $\mathbb{N}$. The sequence $0, 1, 2, \ldots$ is an infinite *descending* chain!
- The greater-than relation $>$ on $\mathbb{N}$.
- The less-than relation $<$ on $\mathbb{Z}$. The sequence $0, -1, -2, \ldots$ is an infinite descending chain.
- The less-than relation $<$ on the real interval $[0, 1]$. $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$ is an infinite descending chain.
- The proper subset relation $\subset$ on arbitrary subsets of $\mathbb{N}$. The sequence $\mathbb{N}, \mathbb{N} - \{0\}, \mathbb{N} - \{0, 1\}, \ldots$ is an infinite descending chain.

3 Well-Founded Induction

For any well-founded binary relation $\prec$ on a set A, the principle of well-founded induction allows us to prove some predicate P holds on all elements of A by proving that, for any $a \in A$ such that $P(b)$ holds whenever $b \prec a$, then $P(a)$ must also hold. In mathematical notation,

$$\forall a \in A.\, (\forall b \in A.\, b \prec a \Longrightarrow P(b)) \Longrightarrow P(a) \quad \Longrightarrow \quad \forall a \in A.\, P(a). \tag{1}$$

The basis for this induction is when a has no $\prec$-predecessors, in which case $\forall b \in A.\, b \prec a \Longrightarrow P(b)$ holds vacuously.

We can see how this generalizes all forms of induction we have seen so far.

Example 1. For the well-founded predecessor relation on $\mathbb{N}$ (pred $= \{(m+1, m) \mid m \in \mathbb{N}\}$), (1) reduces to the standard principle of mathematical induction. Because 0 has no predecessors, $\forall n \in \mathbb{N}.\, (0, n) \in \text{pred} \Longrightarrow P(n)$ hold vacuously, and we must directly prove $P(0)$. For all other natural numbers $n > 0$, $n = m + 1$, so we must prove $P(m) \Longrightarrow P(m+1)$.

Example 2. For the well-founded relation $<$ on $\mathbb{N}$, (1) reduces to *strong* induction on $\mathbb{N}$: to prove $\forall n \in \mathbb{N}.\, P(n)$, it suffices to prove that $P(n)$ holds whenever *all* of $P(0), P(1), \ldots, P(n-1)$ hold. When $n = 0$, the set of inductive hypotheses is empty, requiring a direct proof of $P(0)$.

Example 3. Structural induction on an inductive set is a form of well-founded induction. For instance, the strict sub-term relation on ARITH expression is a well-founded relation where n and x are the base cases, as they have no strict sub-expressions, and each other expression form is an inductive case, as it contains strict sub-expression.

Similarly, structural induction on the step relation $\longrightarrow$ is well founded for the same reason.

3.1 Equivalence of Well-Foundedness and the Validity of Induction

In fact, one can show that the induction principle (1) is valid *if and only if* the relation $\prec$ is well-founded.

Theorem 1. *The induction principle (1) holds for $\prec$ on set A if and only if $\prec$ is well-founded on A.*

Proof. This will be a proof by contradiction.

We first prove that, if principle (1) is not valid for $\prec$ on A, then there is an infinite descending chain (that is, $\prec$ is not well-founded on A). By assumption, (1) does not hold, which means there is some predicate P and some element $a_0 \in A$ such that $\neg P(a_0)$, and yet

$$\forall a \in A.\, (\forall b \in A.\, b \prec a \Longrightarrow P(b)) \Longrightarrow P(a).$$

This implication is equivalent to:

$$\forall a \in A.\, \neg P(a) \Longrightarrow \exists b \in A.\, b \prec a \wedge \neg P(b).$$

Since $\neg P(a_0)$, this means there must be some $a_1 \prec a_0$ such that $\neg P(a_1)$. But because $P(a_1)$ is false, the same logic applies again, giving an $a_2 \prec a_1$ where $\neg P(a_2)$. Using the axiom of dependent choice (a weakened form of the axiom of choice), one can continue this process to construct an infinite descending chain $a_0, a_1, a_2, \ldots$ such that $a_{i+1} \prec a_i$ and $\neg P(a_i)$ for all $i \geq 0$. Therefore $\prec$ is not well-founded on A.

To prove the other direction, we assume there is an infinite descending chain $a_0, a_1, a_2, \ldots$ and show that (1) cannot hold. Specifically, consider the predicate $P(a) = a \notin \{a_0, a_1, a_2, \ldots\}$.

The a_is form an infinite descending chain, so if $\forall b \in A.\, b \prec a \implies P(b)$, that means whenever $b \prec a$ that $b \neq a_i$ for all $i \geq 0$, which must mean $a \notin \{a_0, a_1, a_2, \ldots\}$ as well because otherwise *something* smaller than a would also be in the set. Thus the premise of (1) is satisfied for P, yet it is clearly not the case that $\forall a \in A.\, P(a)$, as $\neg P(a_i)$ for all $i \geq 0$. □

This equivalence is deep and important. It immediately proves the equivalence of the principles of strong mathematical induction on $\mathbb{N}$ and the well-ordering of $\mathbb{N}$—that every non-empty subset of $\mathbb{N}$ has a unique least element, which is straightforwardly the same as $<$ being well-founded on $\mathbb{N}$. It is not too hard to show that $<$ is well-founded on $\mathbb{N}$ if and only if predecessor is well-founded (assuming a standard definition of $<$ in terms of predecessor), which then includes the principle of weak induction on $\mathbb{N}$ as being equivalent to both strong induction and well-ordering.

4 Well-Founded Induction, Structural Induction, and Recursion

Well-founded induction tells us that structural induction works properly and the recursive functions over inductively-defined data exist and are unique.

Take, for instance, the FV definition above. Define $e < e'$ to be when e is a *proper* subterm of e'. That is, e is a subterm of e' and $e \neq e'$. If we think of ARITH expressions as finite labeled trees where the label is which type of term, then e is a subtree of e'. Since the trees are finite, $<$ is well-founded. Fundamentally, this is why structural induction is mathematically sound.

We can now show that $\mathrm{FV}(e)$ is a total function on ARITH expression. In particular, we can prove by induction on e that for every $e \in \mathbf{Exp}$, there is a unique $V \in 2^{\mathbf{Var}}$ such that $(e, V) \in \mathrm{FV}$. The base cases ($e = n$ and $e = x$) are clear from the definition of FV. The three inductive cases follow by applying the inductive hypotheses and noting that $\cup$ and set subtraction have unique results.

Now that we have a strong understanding of what induction is and why it works, we will be using these ideas and principles liberally throughout the rest of the course.