Math 2200-002/Discrete Mathematics

Induction and Well-Ordering

Induction is a tool for proving logical propositions of the form:

$$(\forall n \geq m)P(n)$$

In **simple induction**, you prove the statement above in two stages:

(i) Prove the *base case* $P(m)$.

(ii) Prove the *inductive step* $(\forall k \geq m)(P(k) \to P(k+1))$.

The base case gets the induction started, and by the inductive step:

$$P(m+1), P(m+2), ... \text{ are all true as well.}$$

Example. Prove that for all $n \geq 1$,

$$1 + 2 + \cdots + n = \binom{n+1}{2} = \frac{(n+1)n}{2}$$

Proof. We start with the base case $m = 1$.

(i) $1 = \binom{2}{2}$ is the base case.

(ii) If

$$1 + 2 + \cdots + k = \binom{k+1}{2}$$

then

$$1 + 2 + \cdots + k + (k+1) = \binom{k+1}{2} + (k+1) =$$

$$= \frac{(k+1)k}{2} + (k+1) = \frac{(k+1)k + (k+1)2}{2} = \frac{(k+1)(k+2)}{2} = \binom{k+2}{2}$$

This is the inductive step.

The starting point m can be any integer.

Example. Prove that for all finite sets S, $(|S| = n) \to (|\mathcal{P}(S)| = 2^n)$.

Proof. We start with the base case $m = 0$.

(i) If $|S| = 0$, then $S = \emptyset$, so $\mathcal{P}(S) = \{\emptyset\}$, so $|\mathcal{P}(S)| = 1$ and $1 = 2^0$.

(ii) For the inductive step, assume that $(|S| = k) \to (|\mathcal{P}(S)| = 2^k)$.

Let T be a set with $k+1$ elements, choose $t \in T$ and let $S = T - \{t\}$. Then by assumption, $|\mathcal{P}(S)| = 2^k$. But each subset $A \subset S$ determines **two** subsets of T, namely A itself and $A \cup \{t\}$. Taken all together, these exactly account for **each of** the subsets of T. Thus:

$$|\mathcal{P}(T)| = 2|\mathcal{P}(S)| = 2 \cdot 2^k = 2^{k+1}$$

and the inductive step is established.

There is a variation on this, known as **strong induction**, in which:

(i) The base case $P(m)$ and

(ii) The *strong inductive step*

$$(\forall k \geq m)((P(m) \wedge P(m+1) \wedge \cdots \wedge P(k)) \rightarrow P(k+1))$$

together imply the result:

$$(\forall n \geq m)P(n)$$

This version of induction can be more useful than simple induction.

Example. Every natural number $n \geq 2$ is a product of prime numbers.

Proof. We use strong induction with base case $m = 2$.

(i) $m = 2$ is a prime, so it is a product of primes (namely itself).

(ii) Suppose $2, 3, ..., k$ are each products of primes, and consider $k+1$. Then either:

(a) $k + 1$ is a prime, in which case it is a product of primes, or

(b) $k + 1$ is composite, in which case $k + 1 = ab$ and **both** a and b are in the range $2, 3, ..., k$, so a and b are both products of primes, so their product is also a product of primes.

Both inductions are equivalent to the different-looking:

Well-Ordered Axiom. Let $\mathbb{Z}^{\geq m} = \{n \in \mathbb{Z} \mid n \geq m\}$ and $S \subseteq \mathbb{Z}^{\geq m}$. Then either:

(i) $S = \emptyset$ or

(ii) S has a smallest element.

Like the principles of induction, this is useful for proving things.

Example. (The Division Algorithm for $\mathbb{Z}$) Let $n \in \mathbb{Z}$ and $m \in \mathbb{N}$. Then there is an integer q such that:

$$n = mq + r \text{ and } 0 \leq r < m$$

Proof. Let $S = \{n - mq \mid q \in \mathbb{Z}\} \cap \mathbb{Z}^{\geq 0}$.

Then $S \neq \emptyset$ because $q < n/m$ implies $n - mq > n - m(n/m) = 0$. Therefore S has a smallest element, which we'll call r and note that:

$$n = mq + r \text{ for some integer } q \text{, by definition}$$

But it must be the case that $0 \leq r < m$ because otherwise, $r - m \geq 0$ and then $r - m = n - mq - m = n - m(q + 1) \in S$ would be a smaller element of the set S.

We are ready for the big theorem.

Theorem. Fix $m \in \mathbb{Z}$. Then the following are equivalent:

(a) The well-ordered axiom.

(b) Simple Induction

(c) Strong Induction

Proof. We will prove $(a) \to (b) \to (c) \to (a)$. First, we need to rephrase all these things as logical propositions.

(a) Well-ordered axiom. Let $S \subseteq \mathbb{Z}^{\geq m}$. Then:

$$(S = \emptyset) \vee (\exists s \in S)(\forall t \in S)(t \geq s)$$

(b) Simple induction. Let $P(n)$ be a propositional function. Then:

$$P(m) \wedge (\forall k \geq m)(P(k) \to P(k+1)) \to (\forall n \geq m)P(n)$$

This is unruly, so we'll simplify it using the two equivalences:

$$p \to q \equiv \neg p \vee q \text{ and } \neg(p \to q) \equiv p \wedge \neg q$$

The first equivalence gives:

$$\neg\left(P(m) \wedge (\forall k \geq m)(P(k) \to P(k+1)\right) \vee (\forall n \geq m)P(n)$$

We use DeMorgan's laws and the second equivalence to get:

$$\neg P(m) \vee (\exists k \geq m)(P(k) \wedge \neg P(k+1)) \vee (\forall n \geq m)P(n)$$

This is the version of simple induction that we will use.
(Note: This is three separate propositions with "or" operations)

(c) Strong Induction. Let $P(n)$ be a propositional function. Then:

$$\neg P(m) \vee (\exists k \geq m)(P(m) \wedge \cdots \wedge P(k) \wedge \neg P(k+1)) \vee (\forall n \geq m)P(n)$$

using the same equivalences as in simple induction.

Back to the proof.

(a) $\to$ (b). Given a propositional function $P(n)$, let

$$S = \{n \geq m \mid P(n) \text{ is } \textbf{false}\}$$

By the well-ordered axiom, one of three things is true of S:

- $S = \emptyset$ (in which case $P(n)$ is true for all $n \geq m$).
- $m \in S$, in which case $P(m)$ is **false** or
- $S \neq \emptyset$ and its smallest element s is larger than m. In that case:

$$P(s-1) \text{ is } \textbf{true} \text{ and } P(s) \text{ is } \textbf{false}$$

If we let $k = s - 1 \geq m$, then this is:

$$(\exists k \geq m)(P(k) \wedge \neg P(k+1))$$

These are exactly the three propositions of simple induction!

(b) → (c). Let $P(n)$ be any proposition, and let:

$$Q(n) \equiv P(m) \wedge \cdots \wedge P(n)$$

for all $n \geq m$. Then simple induction for $Q(n)$ is:

$$\neg Q(m) \vee (\exists k \geq m)(Q(k) \wedge \neg Q(k+1)) \vee (\forall n \geq m) Q(n)$$

and full induction for $P(n)$ is:

$$\neg P(m) \vee (\exists k \geq m)(P(m) \wedge \cdots \wedge P(k) \wedge \neg P(k+1)) \vee (\forall n \geq m) P(n)$$

Since $P(m) \equiv Q(m)$ and $(\forall n \geq m) P(m) \equiv (\forall n \geq m) Q(m)$, we only have to compare the third propositions:

$$Q(k) \wedge \neg Q(k+1) \text{ with } P(m) \wedge \cdots \wedge P(k) \wedge \neg P(k+1)$$

But $Q(k) \equiv P(m) \wedge \cdots \wedge P(k)$ and $Q(k+1) = Q(k) \wedge P(k+1)$, so this follows from:

$$p \wedge \neg q \equiv p \wedge \neg(p \wedge q)$$

which can be checked with a truth table. Thus simple induction for $Q(n)$ gives full induction for $P(n)$, and since $P(n)$ was arbitrary, it follows that simple induction implies full induction.

(c) → (a) Suppose $S \subseteq \mathbb{Z}^{\geq n}$, and let:

$$P(n) = \begin{cases} \mathbf{T} \text{ if } n \notin S \\ \\ \mathbf{F} \text{ if } n \in S \end{cases}$$

Then strong induction for $P(n)$ gives one of the following:

- $(\forall n \geq m) P(n)$ (in which case $S = \emptyset$) or
- $\neg P(m)$ (so m is the smallest element of S) or
- $(\exists k \geq m)(P(m) \wedge \cdots \wedge P(k) \wedge \neg P(k+1))$ (so $k+1 \in S$ and $m, ..., k \notin S$, i.e. $k+1$ is the smallest element of S).

In other words, $S = \emptyset$ or S has a smallest element!

Homework. (Each problem is worth two points).

1. Prove by simple induction that $2 + 4 + 6 + \cdots + 2n = (n+1)n$.

2. Prove by simple induction that $2 + 4 + 8 + \cdots + 2^n = 2^{n+1} - 2$.

3. Find all the postage amounts you can make with 4 and 7 cent stamps, and prove your answer with induction.

4. Do Problem 36 on Page 344 (§5.2) of the book.

5. A subset $A \subseteq \mathbb{R}$ is well-ordered if every $S \subseteq A$ is either empty or else has a smallest element. Which of the following sets is well-ordered?

(a) $\mathbb{Z}^{\geq -1}$ (b) $\mathbb{Z}^{\leq 0}$ (c) $\mathbb{Q}^{\geq 0}$ (d) $\{1 - \frac{1}{n} \mid n \in \mathbb{N}\}$ (e) $\{m - \frac{1}{n} \mid m, n \in \mathbb{N}\}$