CMPS 101
Algorithms and Abstract Data Types
Fall 2006

Induction Proofs

Let $P(n)$ be a propositional function, i.e. P is a function whose domain is (some subset of) the set of integers and whose codomain is the set {True, False}. Informally, this means $P(n)$ is a sentence, statement, or assertion whose truth or falsity depends on the integer *n*. *Mathematical Induction* is a proof technique which can be used to prove statements of the form $\forall n \geq n_0 : P(n)$ ("for all *n* greater than or equal to n_0, $P(n)$ is true"), where n_0 is a fixed integer. A proof by Mathematical Induction contains two steps:

I. **Base Step:** Prove directly that the proposition $P(n_0)$ is true.

IIa. **Induction Step:** Prove $\forall n \geq n_0 : (P(n) \rightarrow P(n+1))$.
To do this pick an arbitrary $n \geq n_0$, and assume for this *n* that $P(n)$ is true. Then show as a consequence that $P(n+1)$ is true. The statement $P(n)$ is often called the *induction hypothesis*, since it is what is assumed in the induction step.

When I and II are complete we conclude that $P(n)$ is true for all $n \geq n_0$. Induction is sometimes explained in terms of a domino analogy. Consider an infinite set of dominos which are lined up and ready to fall. Each domino is labeled by a positive integer, starting with n_0. (It is often the case that $n_0 = 1$, which we assume here for the sake of definiteness). Let $P(n)$ be the assertion: "the *n*th domino falls". First prove $P(1)$, i.e. "the first domino falls", then prove $\forall n \geq 1 : (P(n) \rightarrow P(n+1))$ which says "if any particular domino falls, then the next domino must also fall". When this is done we may conclude $\forall n \geq 1 : P(n)$, "all dominos fall". There are a number of variations on the induction step. The first is just a reparametrization of IIa.

IIb. **Induction Step:** Prove $\forall n > n_0 : (P(n-1) \rightarrow P(n))$
Let $n > n_0$, assume $P(n-1)$ is true, then prove $P(n)$ is true.

Forms **IIa** and **IIb** are said to be based on the *first principle of mathematical induction*. The validity of this principle is proved in the appendix of this handout. Another important variation is called the *second principle of mathematical induction*, or *strong induction*.

IIc. **Induction Step:** Prove $\forall n \geq n_0 : ((\forall k \leq n : P(k)) \rightarrow P(n+1))$
Let $n \geq n_0$, assume for all *k* in the range $n_0 \leq k \leq n$ that $P(k)$ is true. Then prove as a consequence that $P(n+1)$ is true. In this case the term *induction hypothesis* refers to the stronger assumption: $\forall k \leq n : P(k)$.

The strong induction form is often reparametrized as in **IIb**:

IId. **Induction Step:** Prove $\forall n > n_0 : ((\forall k < n : P(k)) \to P(n))$

Let $n > n_0$, assume for all k in the range $n_0 \le k < n$, that $P(k)$ is true, then prove as a consequence that $P(n)$ is true. In this case the *induction hypothesis* is $\forall k < n : P(k)$.

In terms of the Domino analogy, the strong induction form IId says we must show: (I) the first domino falls, and (II) for any *n*, if all dominos up to but not including the n^{th} domino fall, then the n^{th} domino falls. From (I) and (II) we may conclude that all dominos fall. Strong Induction is most often parameterized as in IId, and form IIc is uncommon. We present here a number of examples of IIa, IIb, and IId.

Example 1 Prove that for all $n \ge 1$:

$$\boxed{\sum_{i=1}^{n} i^2 \;=\; \frac{n(n+1)(2n+1)}{6}}$$

Proof:
Let $P(n)$ be the boxed equation above. We begin the induction at $n_0 = 1$.

I. **Base step** Clearly $\sum_{i=1}^{1} i^2 = 1 = \frac{1\cdot(1+1)\cdot(2\cdot 1+1)}{6}$, showing that $P(1)$ is true.

IIa. **Induction Step** Let $n \ge 1$ and assume $P(n)$ is true. That is, for this particular value of *n*, the boxed equation holds. Then

$$\begin{aligned}
\sum_{i=1}^{n+1} i^2 &= \sum_{i=1}^{n} i^2 + (n+1)^2 \\
&= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 && \text{(by the induction hypothesis)} \\
&= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\
&= \frac{(n+1)\cdot[(n+1)+1]\cdot[2(n+1)+1]}{6} && \text{(by some algebra)}
\end{aligned}$$

showing that $P(n+1)$ is true.
We conclude that $P(n)$ is true for all $n \ge 1$. ///

When writing an induction proof, always state the induction hypothesis explicitly. Also make note of the point in the proof where the induction hypothesis is used.

Example 2 Let $x \in R$ and $x \ne 1$. Show that for all $n \ge 0$:

$$\boxed{\sum_{i=0}^{n} x^i \;=\; \frac{x^{n+1}-1}{x-1}}$$

Proof:
Here we will use form IIb. Again let $P(n)$ be the boxed equation. We begin the induction at $n_0 = 0$.

I. **Base step** $\sum_{i=0}^{0} x^i = x^0 = 1 = \frac{x-1}{x-1}$, showing that $P(1)$ is true.

IIb. **Induction Step** Let $n > 0$ and assume that $P(n-1)$ is true, i.e. assume for this particular *n* that: $\sum_{i=0}^{n-1} x^i = \frac{x^n - 1}{x-1}$. Then

$$\begin{aligned}\sum_{i=0}^{n} x^i &= \sum_{i=0}^{n-1} x^i + x^n \\ &= \frac{x^n - 1}{x-1} + x^n && \text{(by the induction hypothesis)} \\ &= \frac{x^{n+1} - 1}{x-1} && \text{(by some algebra)}\end{aligned}$$

showing that $P(n)$ is true.

Steps I and II prove that $P(n)$ holds for all $n \geq 0$. ///

Exercise 1 Prove that for all $n \geq 1$: $\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$. Do this using both forms **II**a and IIb.

Often the proposition to be proved is not a formula, but some other type of assertion, like an inequality, as in the following example.

Example 3 Define the function $T(n)$ for $n \in Z^+$ by the recurrence

$$T(n) = \begin{cases} 0 & \text{if } n = 1 \\ T(\lfloor n/2 \rfloor) + 1 & \text{if } n \geq 2 \end{cases}$$

Prove that for all $n \geq 1$, $\boxed{T(n) \leq \lg(n)}$, and therefore $T(n) = O(\lg n)$.

Proof:

Let $P(n)$ be the boxed inequality above.

I. **Base Step**

The inequality $T(1) \leq \lg(1)$ reduces to simply $0 \leq 0$, which is obviously true, so $P(1)$ holds.

IId. **Induction Step** (Strong Induction)

Let $n > 1$ and assume for all *k* in the range $1 \leq k < n$ that $P(k)$ is true, i.e. $T(k) \leq \lg(k)$. In particular when $k = \lfloor n/2 \rfloor$, we have $T(\lfloor n/2 \rfloor) \leq \lg\lfloor n/2 \rfloor$. Therefore

$$\begin{aligned}T(n) &= T(\lfloor n/2 \rfloor) + 1 && \text{(by the definition of } T(n)\text{)} \\ &\leq \lg\lfloor n/2 \rfloor + 1 && \text{(by the induction hypothesis)} \\ &\leq \lg(n/2) + 1 && \text{(since } \lfloor x \rfloor \leq x \text{ for any } x\text{)} \\ &\leq \lg(n) - \lg(2) + 1 \\ &= \lg(n),\end{aligned}$$

showing that $P(n)$ is true.

Therefore $T(n) \leq \lg(n)$ for all $n \geq 1$, as claimed. ///

Exercise 2 Define $S(n)$ for $n \in Z^+$ by the recurrence

$$S(n) = \begin{cases} 0 & \text{if } n = 1 \\ S(\lceil n/2 \rceil) + 1 & \text{if } n \ge 2 \end{cases}$$

Prove that for all $n \ge 1$: $S(n) \ge \lg(n)$, and hence $S(n) = \Omega(\lg n)$.

There are many other variations on the induction technique. Occasionally *double induction* is called for, which involves a modification of both the base and induction steps.

Base Step: Prove $P(n_0)$ and $P(n_0 + 1)$.
Induction Step: Prove $\forall n \ge (n_0 + 2) : (P(n-2) \wedge P(n-1) \rightarrow P(n))$.

When these steps are complete, we conclude $\forall n \ge n_0 : P(n)$. In terms of our domino analogy, we prove: (I) the first two dominos fall, and (II) if any two consecutive dominos fall, then the very next domino falls, and from (I) and (II) we deduce that all dominos fall. The next example uses double induction and concerns the Fibonacci sequence F_n defined by: $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$, i.e. each term in the sequence is the sum of the preceding two. Using this recurrence formula, the first few terms of the Fibonacci sequence are easily computed: $F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, etc.

Example 4 Let $a = \frac{1+\sqrt{5}}{2}$, and $b = \frac{1-\sqrt{5}}{2}$. Prove that for all $n \ge 0$, $\boxed{F_n = \frac{1}{\sqrt{5}}\left[a^n - b^n\right].}$

Proof:
Let $P(n)$ denote the boxed equation above.

I. **Base Step** Observe that $P(0)$ and $P(1)$ are true since $\frac{1}{\sqrt{5}}\left[a^0 - b^0\right] = 0 = F_0$ and $\frac{1}{\sqrt{5}}\left[a^1 - b^1\right] = 1 = F_1$.

II. **Induction Step** Let $n \ge 2$ and assume that both $P(n-2)$ and $P(n-1)$ are true, i.e. we assume for this *n* that

$$F_{n-2} = \frac{1}{\sqrt{5}}\left[a^{n-2} - b^{n-2}\right] \quad \text{and} \quad F_{n-1} = \frac{1}{\sqrt{5}}\left[a^{n-1} - b^{n-1}\right].$$

The induction hypothesis yields

$$F_n = F_{n-1} + F_{n-2} = \frac{1}{\sqrt{5}}\left[a^{n-2}(a+1) - b^{n-2}(b+1)\right].$$

One checks that *a* and *b* are roots of the quadratic equation $x^2 - x - 1 = 0$, whence $a^2 = a + 1$, and $b^2 = b + 1$. Therefore

$$F_n = \frac{1}{\sqrt{5}}\left[a^{n-2} \cdot a^2 - b^{n-2} \cdot b^2\right] = \frac{1}{\sqrt{5}}\left[a^n - b^n\right],$$

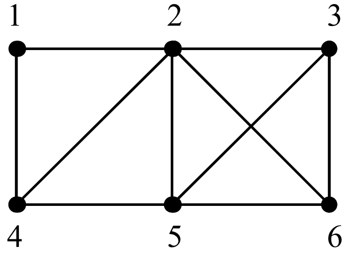
showing that $P(n)$ is true.

Together (I) and (II) imply that $F_n = \frac{1}{\sqrt{5}}\left[a^n - b^n\right]$ for all $n \ge 0$. ///

Exercise 3 Let F_n be the Fibonacci sequence and define *a* as above. Show that $F_n \geq a^{n-2}$ for all $n \geq 2$, and hence $F_n = \Omega(a^n)$. (Prove this by double induction, not as a consequence of the last example.)

A Short Introduction to Graphs

Often the propositional function $P(n)$ is some assertion concerning other types of mathematical structures, such as graphs, or trees. A *graph G* is a pair of sets $G = (V, E)$. The elements of $V \neq \varnothing$ are called *vertices*, and the elements of *E* are called *edges*. Each edge joins two distinct vertices, called it's *ends*, and no two edges have the same ends. Abstractly, an edge is an unordered pair of vertices, i.e. a 2-element subset of *V*. Two vertices that are joined by an edge are said to be *adjacent*, and an edge is said to be *incident* with it's two end vertices. Two edges are said to be *adjacent* if they are incident with a common end vertex. Thus in the example below: vertex 1 is adjacent to vertex 4, vertex 2 is incident with edge 26, and edge 45 is adjacent to edge 53.

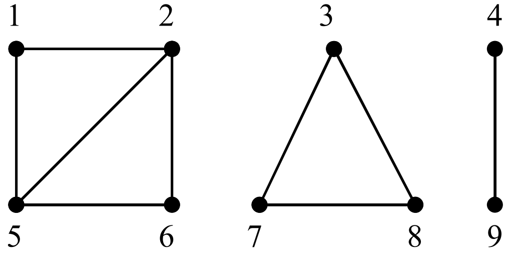


V = {1, 2, 3, 4, 5, 6} *E* = {12, 14, 23, 24, 25, 26, 35, 36, 45, 56}

Let $x, y \in V$. An *x-y path* in *G* is a sequence of vertices starting with *x* and ending with *y*, in which each consecutive pair of vertices are adjacent. We require that all vertices other than *x* and *y* be distinct. If $x = y$, i.e. if the initial and terminal vertices in a path are identical, then the path is called a *cycle*. The *length* of a path is the number of edges traversed by the sequence. In the above example we have:

A 1-6 path of length 5: 1, 2, 4, 5, 3, 6
A 1-6 path of length 3: 1, 4, 5, 6
Another 1-6 path of length 3: 1, 2, 3, 6
A cycle of length 6: 1, 2, 6, 3, 5, 4, 1
A cycle of length 3: 6, 2, 5, 6

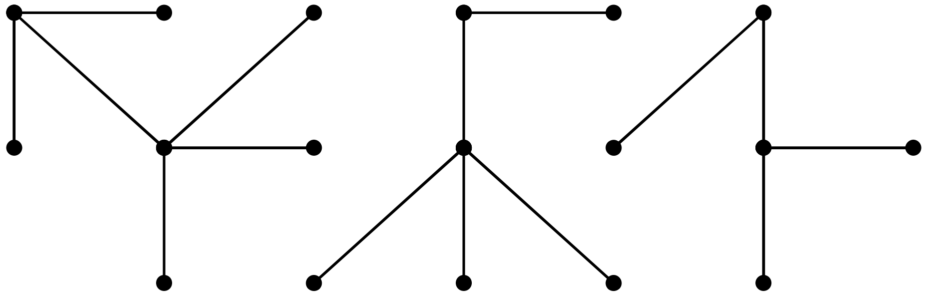
A graph is said to be *connected* if it contains an *x-y* path for every $x, y \in V$, otherwise it is called *disconnected*. The example above is clearly connected, while the following example is disconnected.



V = {1, 2, 3, 4, 5, 6, 7, 8, 9} *E* = {12, 15, 25, 26, 56, 37, 38, 78, 49}

A *subgraph* of a graph *G* is a graph *H* in which $V(H) \subseteq V(G)$, and $E(H) \subseteq E(G)$. In the above example ({1, 2, 5}, {12, 15, 25}) is a connected subgraph, while ({2, 3, 6, 7}, {26, 37}) is a disconnected subgraph. A subgraph *H* is called a *connected component* of *G* if it is (i) connected, and (ii) maximal with respect to property (i), i.e. any other subgraph of G that contains H is disconnected. The above example clearly has three connected components: ({1, 2, 5, 6}, {12, 15, 25, 26, 56}), ({3, 7, 8}, {37, 38, 78}), and ({4, 9}, {49}). Obviously a graph is connected if and only if it has exactly one connected component.

A graph G is called *acyclic* if it contains no cycles. A *tree* is a graph that is both connected and acyclic. The connected components of an acyclic graph are obviously trees. For this reason an acyclic graph is sometimes called a *forest*. The following graph is a forest with three connected components.



Observe that the number of vertices in each tree in this forest is one less that the number of vertices. This is true for all trees, as we now show.

Example 5 For all $n \geq 1$, $\boxed{\text{if } T \text{ is a tree on } n \text{ vertices, then } T \text{ contains } n-1 \text{ edges.}}$

Proof:
Let $P(n)$ be the boxed statement above. We begin at $n_0 = 1$, and use the strong induction form IId.

I. Base step
If T has just one vertex, then it can have no edges, since in the definition of a graph, each edge must have distinct end vertices. Therefore $P(1)$ holds.

IId. Induction Step
Let $n > 1$ and assume for all k in the range $1 \leq k < n$, that $P(k)$ is true, i.e. for any such k, all trees on k vertices contain $k-1$ edges. Now let T be a tree on n vertices, pick any edge e in T, and remove it. The removal of e splits T into two subtrees, each having fewer than n vertices. (This follows from some elementary facts about graphs which we omit for the sake of brevity.) Suppose for the sake of definiteness that the two subtrees have k_1 and k_2 vertices, respectively. Since no vertices were removed, we must have $k_1 + k_2 = n$. By our inductive hypothesis, these two subtrees have $k_1 - 1$ and $k_2 - 1$ edges, respectively. Upon replacing the edge e, we see that the number of edges originally in T must have been $(k_1 - 1) + (k_2 - 1) + 1 = k_1 + k_2 - 1 = n - 1$, as required.

By the second principle of mathematical induction, all trees on n vertices have $n-1$ edges. ///

Induction Fallacies
The next three examples illustrate some pitfalls to be avoided when constructing induction proofs. The result in Example A was proved correctly in Example 5. Here we give an invalid proof of the same fact that illustrates an argument which some authors have called "the induction trap".

Example A For all $n \geq 1$, if T is a tree on n vertices then T has $n-1$ edges.

Proof: (Invalid)
Base Step: If $n = 1$ then T has no edges, since each edge must have distinct end vertices.
Induction Step: Let $n \geq 1$ and let T be a tree on n vertices. Assume that T has $n-1$ edges. Add a new vertex and join it to T with a new edge. To be precise, the new edge has the new vertex at one end, and the other end can be any existing vertex in T. The resulting graph has $n+1$ vertices and n edges, and is clearly a tree since connectedness is maintained and no cycles were created. By the principle of mathematical induction, all trees on n vertices have $n-1$ edges. □

First note that the base step is identical to that in Example 5, and is correct. For the induction step, the argument attempts to follow IIa, but does not do so. In this example $P(n)$ is of the form $A(n) \to B(n)$ where $A(n)$ is the statement "T is a tree on n vertices", and $B(n)$ is "T has $n-1$ edges". The induction step should therefore be to prove, for all $n \geq 1$, that $P(n) \to P(n+1)$, i.e.

$$(A(n) \to B(n)) \to (A(n+1) \to B(n+1)).$$

To prove this, we should assume $A(n) \to B(n)$, then assume $A(n+1)$, then show as a consequence that $B(n+1)$ is true. In other words we should:

- Assume all trees on n vertices have $n-1$ edges
- Assume T has $n+1$ vertices
- Show as a consequence that T has n edges

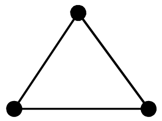
The argument did not follow this format however. Instead it does the following.

- Assume T has n vertices
- Assume T has $n-1$ edges
- Construct a new tree from T having $n+1$ vertices and n edges

Therefore the argument was not a proof by induction. Some students would nevertheless hold that the argument is still valid, even though it is not a true induction proof. The next example shows convincingly that it cannot be valid.

Example B For all $n \geq 1$, if G is a connected graph on n vertices, then G has $n-1$ edges. (**False!**)

We notice right away that the above statement is false, since the graph below provides an elementary counter-example. But consider the following "proof" in light of Example A.



Proof: (Invalid)
Base Step: If $n = 1$ then G has no edges, since each edge must have distinct end vertices.
Induction Step: Let $n \geq 1$ and let G be a connected graph on n vertices. Assume that G has $n-1$ edges. Add a new vertex and join it to G with a new edge. The resulting graph has $n+1$ vertices and n edges, and is clearly connected. By the principle of mathematical induction, all connected graphs on n vertices have $n-1$ edges. □

Observe that Example B follows the format of Example A exactly. Thus if A is valid, so must B be valid. But the assertion "proved" in B is false! Therefore B cannot be a valid argument, and so neither is A.

Example C All horses are of the same color.

Proof: (Invalid)
We prove that for all $n \geq 1$: $\boxed{\text{if } S \text{ is a set of } n \text{ horses, then all horses in } S \text{ have the same color.}}$ The result follows on letting *S* be the set of all horses. Let $P(n)$ be the boxed statement, and proceed by induction on *n*.

Base Step: Let $n = 1$. Obviously if *S* is a set consisting of just one horse, then all horses in *S* must have the same color. Thus $P(1)$ is true.
Induction Step: Let $n > 1$ and assume that in any set of *n* horses, all horses are of the same color. Let *S* be a set of $n+1$ horses, say $S = \{h_1, h_2, h_3, \ldots, h_{n+1}\}$. Then the sets

$$S' = \{h_2, h_3, \ldots, h_{n+1}\} = S - \{h_1\}$$

and

$$S'' = \{h_1, h_3, \ldots, h_{n+1}\} = S - \{h_2\}$$

each contain exactly *n* horses, and so by the induction hypothesis all horses in S' are of one color, and likewise for S''. Observe that $h_3 \in S' \cap S''$ and that h_3 can have only one color. Therefore the color of the horses in S' is identical to that of the horses in S''. (Note $n > 1 \Rightarrow n \geq 2 \Rightarrow n+1 \geq 3$, so there is in fact a third horse, and he can have only one color.) Since $S = S' \cup S''$ it follows that all horses in *S* are of the same color. Thus $P(n+1)$ is true, showing that $P(n) \to P(n+1)$ for all $n > 1$. The result now follows by induction. □

Obviously the proposition being proved is false, so there is something wrong with the proof, but what? The base step is certainly correct, and the induction step, as stated, is also correct. The problem is that the induction step was not quantified properly. We should have proved $\forall n \geq 1: P(n) \to P(n+1)$ Instead we proved (correctly) that $\forall n > 1: P(n) \to P(n+1)$. Indeed it is true that $P(2) \to P(3)$, $P(3) \to P(4)$, and $P(4) \to P(5)$, etc., but we never proved (and it is false that) $P(1) \to P(2)$. In terms of the domino analogy, it is as if the first domino falls; and if any domino indexed 2 or above were to fall, then the next domino would fall; but the first domino is not sufficient to topple the second domino, and hence no domino other than the first actually falls.

Justification of the Induction Principles
Here we prove the validity of the first and second principles of mathematical induction. Both proofs are based on the *well ordering property* of the positive integers Z^+, which says: *Any non-empty set of positive integers contains a least element.* We assume this property without proof.

Theorem 1 (weak induction form IIb)
For any propositional function $P(n)$ defined on the positive integers, the following sentence is true:

$$\left[P(1) \wedge \left(\forall n > 1: P(n-1) \to P(n)\right)\right] \to \forall n \geq 1: P(n)$$

Proof:
Assume that $P(1)$ and $\forall n > 1: P(n-1) \to P(n)$ are both true. Let $S = \{n \in Z^+ \mid P(n) \text{ is false}\}$. It is sufficient to show that $S = \varnothing$, since then $P(n)$ is true for all $n \geq 1$. Assume, to get a contradiction, that

$S \neq \varnothing$. Then, by the well ordering property of Z^+, *S* contains a least element, call it *m*. Since $P(1)$ is true, we have $1 \notin S$. Therefore $m > 1$, and $m-1$ is a positive integer. Since *m* is the smallest element in *S*, we must have $m-1 \notin S$, whence $P(m-1)$ is true. We have assumed for all $n > 1$ that $P(n-1) \to P(n)$ is true. In particular for $n = m$, we have $P(m-1) \to P(m)$. Since both $P(m-1)$ and $P(m-1) \to P(m)$ are true, we must conclude that $P(m)$ is also true. Thus $m \notin S$, contradicting the very definition of *m* as the smallest element *in S*. Thus our assumption was false, and hence $S = \varnothing$ as required. ///

Theorem 2 (strong induction form IId)
For any propositional function $P(n)$ defined on the positive integers, the following sentence is true:

$$\left[P(1) \wedge \left(\forall n > 1 : \left(\forall k < n : P(k)\right) \to P(n)\right)\right] \to \forall n \geq 1 : P(n)$$

Proof:
Assume $P(1)$ and $\forall n > 1 : \left(\forall k < n : P(k)\right) \to P(n)$ are true, and again let $S = \{\, n \in Z^+ \mid P(n) \text{ is false} \,\}$. As before we show $S = \varnothing$, hence $P(n)$ is true for all $n \geq 1$. Assume that $S \neq \varnothing$. By the well ordering property, *S* contains a least element *m*. Since $P(1)$ is true, we have $1 \notin S$. Therefore $m > 1$, and $m - 1 \geq 1$. Since *m* is the smallest element in *S*, we have for any *k* in the range $1 \leq k \leq m-1$ that $k \notin S$, whence $P(k)$ is true. In other words, $\forall k < m : P(k)$ is true. Now we have also assumed for all $n > 1$, that $\left(\forall k < n : P(k)\right) \to P(n)$ is true. In particular, when $n = m$, we have $\left(\forall k < m : P(k)\right) \to P(m)$. Since both $\forall k < m : P(k)$ and $\left(\forall k < m : P(k)\right) \to P(m)$ are true, we conclude $P(m)$ is also true. Thus $m \notin S$, again contradicting the definition of *m* as the smallest element *in S*. Our assumption was therefore false, and hence $S = \varnothing$ as required. ///

Although we proved both theorems independently, it is possible to show that each implies the other, i.e. theorems 1 and 2 are logically equivalent (exercise). In fact both theorems are equivalent to the well ordering property of the positive integers (exercise.) The terms "strong" and "weak" induction are therefore in some sense misnomers, since neither theorem is really stronger than the other. The term "strong induction" refers instead to the stronger assumption being made in the induction step: $\forall k < n : P(k)$ as opposed to $P(n-1)$.