

Section 4.4 Inductive Proof

What do we believe about nonempty subsets of \mathbf{N} ? Since $\langle \mathbf{N}, < \rangle$ is well-founded, and in fact it is linear, it follows that every nonempty subset has a least element. This little observation is the only thing we need to present the ideas of inductive proof.

Basis for the Principle of Mathematical Induction (PMI)

Let $S \subset \mathbf{N}$, $0 \in S$, and suppose also that $k \in S$ implies $k + 1 \in S$. Then $S = \mathbf{N}$.

Proof. Assume, BWOC, that $S \neq \mathbf{N}$. Then $\mathbf{N} - S$ has a least element x . Since $0 \in S$ and $x \notin S$, it follows that $x > 0$. Since x is the least element of $\mathbf{N} - S$, it follows that $x - 1 \in S$. So the hypothesis tells us that $(x - 1) + 1 \in S$. So we have $x \notin S$ and $x \in S$, a contradiction. Therefore $S = \mathbf{N}$. QED.

Principle of Mathematical Induction (PMI)

Let $P(n)$ denote a statement for each $n \in \mathbf{N}$. To prove $P(n)$ is true for each $n \in \mathbf{N}$ do the following steps.

1. Show $P(0)$ is true.
2. Show that if $P(k)$ is true then $P(k + 1)$ is true.

Proof. Assume that the two steps have been shown. Let $S = \{n \mid P(n) \text{ is true}\}$. Since $P(0)$ is true, it follows that $0 \in S$. Since $P(k)$ true implies $P(k + 1)$ true, it follows that $k \in S$ implies $k + 1 \in S$. So by the Basis for PMI we have $S = \mathbf{N}$. QED.

Remark. PMI also works for statements $P(n)$ where $n \in \{m, m + 1, \dots\}$. In this case, the least element is m , so step 1 is modified to show that $P(m)$ is true.

Example. Prove that $1 + 2 + \dots + n = n(n + 1)/2$ for all $n \in \mathbf{N}$.

Proof. Let $P(n)$ be the given equation. For $n = 0$ the equation is $0 = 0(0 + 1)/2$. So $P(0)$ is true. Now assume $P(k)$ is true and prove $P(k + 1)$ is true. The left side of $P(k + 1)$ is:

$$\begin{aligned} 1 + 2 + \dots + k + (k + 1) &= (1 + 2 + \dots + k) + (k + 1) \\ &= k(k + 1)/2 + (k + 1) && \text{(induction assumption)} \\ &= (k + 1)((k + 1) + 1)/2 && \text{(algebra)} \end{aligned}$$

which is the right side of $P(k + 1)$. So $P(k + 1)$ is true and it follows from PMI that $P(n)$ is true for all $n \in \mathbf{N}$. QED.

Example. Prove that $1^3 + 2^3 + \dots + n^3 = (1 + 2 + \dots + n)^2$ for all $n \in \mathbf{N}$.

Proof. Let $P(n)$ be the given equation. For $n = 0$ the equation is $0^3 = 0^2$. So $P(0)$ is true. Now assume $P(k)$ is true and prove $P(k + 1)$ is true. The left side of $P(k + 1)$ is:

$$\begin{aligned} 1^3 + 2^3 + \dots + k^3 + (k + 1)^3 &= (1^3 + 2^3 + \dots + k^3) + (k + 1)^3 \\ &= (1 + 2 + \dots + k)^2 + (k + 1)^3 && \text{(induction assumption)} \\ &= (k(k + 1)/2)^2 + (k + 1)^3 && \text{(previous example)} \\ &= (k^2 + 4k + 4)(k + 1)^2/4 && \text{(algebra)} \\ &= ((k + 1)(k + 2)/2)^2 && \text{(algebra)} \\ &= (1 + 2 + \dots + (k + 1))^2 && \text{(previous example)} \end{aligned}$$

which is the right side of $P(k + 1)$. So $P(k + 1)$ is true and it follows from PMI that $P(n)$ is true for all $n \in \mathbf{N}$. QED.

Example. Let $f : \mathbf{N} \rightarrow \mathbf{N}$ be defined by $f(n) = \text{if } n = 0 \text{ then } 0 \text{ else } f(n - 1) + n^2$.

Claim: $f(n) = n(n + 1)(2n + 1)/6$ for all $n \in \mathbf{N}$.

Proof. Let $P(n)$ be the given equation. Since $f(0) = 0 = 0(0 + 1)(2 \cdot 0 + 1)/6$, $P(0)$ is true. Now assume $P(k)$ is true and prove $P(k + 1)$ is true. The left side of $P(k + 1)$ is:

$$\begin{aligned} f(k + 1) &= f(k + 1 - 1) + (k + 1)^2 && \text{(definition of } f) \\ &= f(k) + (k + 1)^2 && \text{(algebra)} \\ &= k(k + 1)(2k + 1)/6 + (k + 1)^2 && \text{(induction assumption)} \\ &= (k + 1)(2k^2 + 7k + 6)/6 && \text{(algebra)} \\ &= (k + 1)(k + 2)(2k + 3)/6 && \text{(algebra)} \\ &= (k + 1)((k + 1) + 1)(2(k + 1) + 1)/6 && \text{(algebra)} \end{aligned}$$

which is the right side of $P(k + 1)$. So $P(k + 1)$ is true and it follows from PMI that $P(n)$ is true for all $n \in \mathbf{N}$. QED.

Extending Inductive Proof to Well-Founded Sets

A more general form of inductive proof is based on the following statements about well-founded sets.

Basis for Well-Founded Induction

Let W be a well-founded set. Let S be a subset of W that contains the minimal elements of W and whenever an element $x \in W$ has the property that all its predecessors are in S , then $x \in S$. Then $S = W$.

Proof. Assume, BWOC, that $S \neq W$. Then $W - S$ has a minimal element x . So any predecessor of x must be in S . But the assumption then tells us that $x \in S$. So we have $x \notin S$ and $x \in S$, a contradiction. Therefore $S = W$. QED.

Well-Founded Induction

Let W be a well-founded set. Let $P(x)$ denote a statement for each $x \in W$. To prove $P(x)$ is true for each $x \in W$ do the following steps.

1. Show $P(m)$ is true for each minimal element m of W .
2. Show that if $x \in W$ and $P(y)$ is true for all predecessors y of x , then $P(x)$ is true.

Proof. Assume that the two steps have been shown. Let $S = \{x \in W \mid P(x) \text{ is true}\}$. Since $P(m)$ is true for the minimal elements of W , it follows that S contains the minimal elements of W . The second step tells us that if $x \in W$ and $P(y)$ is true for each $y < x$, then $P(x)$ true. In other words, $x \in W$ and each predecessor of x is in S , then $x \in S$. So by the Basis for Well-founded induction we have $S = W$. QED.

Example (Well-Founded Induction). Let $f : \mathbf{N} \rightarrow \mathbf{N}$ be defined by

$$f(0) = f(1) = 0$$

$$f(n) = f(n - 2) + 1 \text{ (for } n > 1\text{)}.$$

Prove that $f(n) = \lfloor n/2 \rfloor$ for all $n \in \mathbf{N}$.

Proof. In this case, we can use a well-founded ordering of \mathbf{N} that has 0 and 1 as the two minimal elements and with the usual ordering for every other number in \mathbf{N} . The poset diagram at right indicates this ordering.



Let $P(n)$ be the statement “ $f(n) = \lfloor n/2 \rfloor$ ”. The definition of f tells us that $f(0) = f(1) = 0$ and the definition of floor tells us that $\lfloor 0/2 \rfloor = \lfloor 1/2 \rfloor = 0$. So $f(0) = \lfloor 0/2 \rfloor$ and $f(1) = \lfloor 1/2 \rfloor$, which tells us that $P(0)$ and $P(1)$ are true. This takes care of the minimal elements. Now assume that $k > 1$ and $P(i)$ is true (i.e., $f(i) = \lfloor i/2 \rfloor$) for each predecessor $i < k$. We must show that $P(k)$ is true (i.e., $f(k) = \lfloor k/2 \rfloor$). We have the following equations:

$$\begin{aligned} f(k) &= f(k - 2) + 1 && \text{(definition of } f\text{)} \\ &= \lfloor (k - 2)/2 \rfloor + 1 && \text{(induction assumption since } k - 2 < k\text{)} \\ &= \lfloor (k/2) - 1 \rfloor + 1 && \text{(algebra)} \\ &= \lfloor (k/2) \rfloor - 1 + 1 && \text{(property of floor)} \\ &= \lfloor (k/2) \rfloor \end{aligned}$$

So $P(k)$ is true and it follows by well-founded induction that $P(n)$ is true for all $n \in \mathbf{N}$. QED.

A popular corollary to well-founded induction is the *second principle of mathematical induction*.

Second PMI

Let $P(n)$ denote a statement for each $n \in \mathbf{N}$. To prove $P(n)$ is true for each $n \in \mathbf{N}$ do the following steps.

1. Show $P(0)$ is true.
2. Show that if $k > 0$ and $P(i)$ is true for $i < k$ then $P(k)$ is true.

Remark. Second PMI also works for statements $P(n)$ where $n \in \{m, m + 1, \dots\}$. In this case, the least element is m , so step 1 is modified to show that $P(m)$ is true and step 2 is modified to assume $k > m$.

Proof. \mathbf{N} is well-founded with minimal element 0. So the result follows from the well-founded induction theorem. QED.

Example. Prove that every natural number greater than 1 is prime or a sum of primes.

Proof. Let $P(n)$ mean that n is a prime or a sum of primes. We need to show $P(n)$ is true for every $n \geq 2$. Since 2 is prime, $P(2)$ is true. Assume $k > 2$ and $P(i)$ is true for $i < k$. Show $P(k)$ is true. If k is prime, then $P(k)$ is true. Otherwise, $k = ij$ where

$$2 \leq i < k \text{ and } 2 \leq j < k.$$

So by assumption $P(i)$ and $P(j)$ are true. i.e., i and j are primes or sums of primes. But we can write $k = ij = j + j + \dots + j$ (i times), so k is a sum of primes. Thus $P(k)$ is true and it follows from Second PMI that $P(n)$ is true for all $n \geq 2$. QED.

Example. Let $L = \{a^m c^n b^m \mid m, n \in \mathbf{N}\}$. Prove that L is the language of the grammar

$$S \rightarrow aSb \mid T$$

$$T \rightarrow cT \mid \Lambda.$$

Proof. Let M be the language of the grammar. We must show that $L = M$. **First show $L \subset M$.** Let $P(m, n)$ be “Some derivation produces $a^m c^n b^m$.” Let $(x_1, x_2) < (y_1, y_2)$ iff $x_1 + x_2 < y_1 + y_2$. This order is well-founded with minimal element $(0, 0)$. $P(0, 0)$ is true because $S \Rightarrow T \Rightarrow \Lambda$. Assume $(m, n) > (0, 0)$ and $P(i, j)$ is true for all $(i, j) < (m, n)$. Show $P(m, n)$ is true. We have either $m > 0$ or $n > 0$. If $m > 0$, then $(m - 1, n) < (m, n)$. So by assumption $P(m - 1, n)$ is true. So there is a derivation $S \Rightarrow^+ a^{m-1} c^n b^{m-1}$. To derive $a^m c^n b^m$ start with $S \Rightarrow aSb$ and follow it with the steps in $S \Rightarrow^+ a^{m-1} c^n b^{m-1}$. So $P(m, n)$ is true. If $n > 0$, then $(m, n - 1) < (m, n)$. So by assumption $P(m, n - 1)$ is true. So there is a derivation $S \Rightarrow^+ a^m c^{n-1} b^m$. Notice that a terminal string can be derived only by using the production $T \rightarrow \Lambda$ in the last step. If we replace the last step of $S \Rightarrow^+ a^m c^{n-1} b^m$ by two steps that use $T \rightarrow cT$ followed by $T \rightarrow \Lambda$, then we obtain a derivation of $a^m c^n b^m$. So $P(m, n)$ is true. Therefore, $P(m, n)$ is true for all $m, n \in \mathbf{N}$ (by well-founded induction). In other words, $L \subset M$.

Show $M \subset L$. Let $P(n)$ be “Any derivation of length n derives a string in L .” The shortest derivation has length 2 and it is $S \Rightarrow T \Rightarrow \Lambda \in L$. So $P(2)$ is true. Assume $k > 2$ and $P(k)$ is true. Prove that $P(k + 1)$ is true. Any derivation of length $k + 1$ must start with either $S \Rightarrow aSb$ or $S \Rightarrow T$. In the first case, $S \Rightarrow aSb \Rightarrow^+ ayb$ where $S \Rightarrow^+ y$ has length k . Since $P(k)$ is true, it follows that $y \in L$. Therefore, $ayb \in L$. In the second case, $S \Rightarrow T \Rightarrow cT \Rightarrow^+ cy$ where $T \Rightarrow^+ y$ has length $k - 1$. So the derivation $S \Rightarrow T \Rightarrow^+ y$ has length k . Since $P(k)$ is true, it follows that $y \in L$. This derivation does not use $S \rightarrow aSb$, so y must be a string of c 's. Therefore, $cy \in L$. So $P(k + 1)$ is true. Therefore, $P(n)$ is true for all $n \geq 2$ (by PMI). So $M \subset L$. Since $L \subset M$ and $M \subset L$, we have the desired result, $L = M$. QED.