5.2 Strong Induction and Well-Ordering

Sometimes it is easier to prove propositions using a different, yet equivalent, form of mathematical induction, called *strong induction.*

Strong Induction

For proving $\forall n \in \mathbb{Z}^+, P(n)$, we use two steps:

1. BASIS STEP Prove $P(1)$.
2. INDUCTIVE STEP Prove that for every $k \in \mathbb{Z}^+$, if $P(1), P(2), P(3), \ldots, P(k)$ are *all* true (the inductive hypothesis), then $P(k+1)$ is true.

Theorem (Fundamental Theorem of Arithmetic)**.** *Every integer n greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.*

Proof. We will use a proof by contradiction to show that there can be at most one factorization of n into primes in nondecreasing order.

Suppose that the positive integer n can be written as the product of primes in two different ways, say, $n = p_1 p_2 \cdots p_s$ and $n = q_1 q_2 \cdots q_t$, each p_i and q_j are primes such that $p_1 \leq p_2 \leq \cdots \leq p_s$ and $q_1 \leq q_2 \leq \cdots \leq q_t$. When we remove all common primes from the two factorizations, we have

$$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v},$$

where no prime occurs on both sides of this equation and u and v are positive integers. A corollary in §4.3 states that if p is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i. It follows that p_{i_1} divides q_{j_k} for some k. Because no prime divides another prime, this is impossible. Consequently, there can be at most one factorization of n into primes in nondecreasing order.

Now, using mathematical induction, we show that there can be at least one factorization of n into primes in nondecreasing order.

Let $P(n)$ be the proposition that n can be written as the product of primes.

1. BASIS STEP: $P(2)$ is true, because 2 can be written as the product of one prime, itself.
2. INDUCTIVE STEP: The inductive hypothesis is the assumption that $P(j)$ is true for all integers j with $2 \leq j \leq k$, that is, the assumption that j can be written as the product of primes whenever j is a positive integer at least 2 and not exceeding k. To complete the inductive step, we must show that $P(k+1)$ is true under this assumption, that is, that $k+1$ is the product of primes.

   There are two cases to consider, namely, when $k+1$ is prime and when $k+1$ is composite. If $k+1$ is prime, we immediately see that $P(k+1)$ is true. Otherwise, $k+1$ is composite and can be written as the product of two positive integers a and b with $2 \leq a \leq b < k+1$. Because both a and b are integers at least 2 and not exceeding k, we can use the inductive hypothesis to write both a and b as the product of primes. Thus, if $k+1$ is composite, we can write it as the product of primes, namely, those primes in the factorization of a and those in the factorization of b.

Since there can be at most one factorization and at least one factorization into primes, the uniqueness of the factorization of n into primes follows. □

Well-Ordering Property (WOP)

The validity of both the principle of mathematical induction and strong induction follows from a fundamental axiom of the set of integers, the well-ordering property. The well-ordering property states that every nonempty set of nonnegative integers has a least element. We will show how we can directly use the well-ordering property in proofs.

The Well-Ordering Property is an axiom about $\mathbb{Z}^+$ that we *assume* to be true. Appendix 1 in textbook has the following four axioms about $\mathbb{Z}^+$:

1. The number 1 is a positive integer.
2. If $n \in \mathbb{Z}^+$, then $n+1$, the successor of n, is also a positive integer.
3. Every positive integer other than 1 is the successor of a positive integer.
4. (The Well-Ordering Property) Every nonempty subset of the set of positive integers has a least element.

Thus we can use the Well-Ordering Property as a tool in proofs.

Theorem (THE DIVISION ALGORITHM)**.** *Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.*

Proof. Let S be the set of nonnegative integers of the form $a - dq$, where q is an integer. This set is nonempty because $-dq$ can be made as large as desired (taking q to be a negative integer with large absolute value). By the well-ordering property, S has a least element $r = a - dq_0$. The integer r is nonnegative. It is also the case that $r < d$. If it were not, then there would be a smaller nonnegative element in S, namely, $a - d(q_0 + 1)$. To see this, suppose that $r \geq d$. Because $a = dq_0 + r$, it follows that $a - d(q_0 + 1) = (a - dq_0) - d = r - d \geq 0$. Consequently, there are integers q and r with $0 \leq r < d$.

The proof that q and r are unique:

Suppose that we have two such pairs, say (q, r) and (q', r'), so that $a = dq + r = dq' + r'$, with $0 \leq r, r' < d$. We will show that the pairs are really the same, that is, $q = q'$ and $r = r'$.

$$dq + r = dq' + r' \Rightarrow d(q - q') = r' - r.$$

Therefore $d \mid (r' - r)$.

$$(0 \leq r < d) \wedge (0 \leq r' < d) \Rightarrow |r' - r| < d.$$

The only multiple of d in that range is 0, so we are forced to conclude that $r' = r$.

To show that $q = q'$:

$$q = \frac{a - r}{d} = \frac{a - r'}{d} = q'. \qquad \square$$

We can show that the well-ordering property, the principle of mathematical induction, and strong induction are all equivalent. That is, the validity of each of these three proof techniques implies the validity of the other two techniques.

Theorem 1. *Mathematical induction $\Rightarrow$ the well-ordering property.*

Proof. We prove this by contradiction. Suppose that the well-ordering property were false. Let S be a counterexample: a nonempty set of nonnegative integers that contains no smallest element. Let $P(n)$ be the statement "$i \notin S$ for all $i \leq n$." We will show that $P(n)$ is true for all n (which will contradict the assertion that S is nonempty). Now $P(0)$ must be true, because if $0 \in S$ then clearly S would have a smallest element, namely 0. Suppose now that $P(n)$ is true, so that $i \notin S$ for all $i = 0, 1, 2, \ldots, n$. We must show that $P(n+1)$ is true, which amounts to showing that $n + 1 \notin S$. If $n + 1 \in S$, then $n + 1$ would be the smallest element of S, and this would contradict our assumption. Therefore $n + 1 \notin S$. Thus we have shown by the principle of mathematical induction that $P(n)$ is true for all n, which means that there can be no elements of S. This contradicts our assumption that $S \neq \emptyset$, and our proof by contradiction is complete. $\square$

Theorem 2. *The well-ordering property $\Rightarrow$ strong induction.*

Proof. To show that strong induction is valid, let us suppose that we have a proposition $\forall n, P(n)$ that has been proved using it. We must show that in fact $\forall n, P(n)$ is true (to say that a principle of proof is valid means that it proves only true propositions). Let S be the set of counterexamples, i.e, $S = \{n \mid \neg P(n)\}$. We want to show that $S = \emptyset$. We argue by contradiction. Assume that $S \neq \emptyset$. Then by the well-ordering property, S has a smallest element. Since part of the method of strong induction is to show that $P(1)$ is true, this smallest counterexample must be greater than 1. Let us call it $k+1$. Since $k+1$ is the smallest element of S, it must be the case that $P(1) \wedge P(2) \wedge \cdots \wedge P(k)$ is true. But the rest of the proof using strong induction involved showing that $P(1) \wedge P(2) \wedge \cdots \wedge P(k)$ implied $P(k+1)$; therefore since the hypothesis is true, the conclusion must be true as well, i.e., $P(k+1)$ is true. This contradicts our assumption that $k+1 \in S$. Therefore we conclude that $S = \emptyset$, so $\forall n, P(n)$ is true. □

Theorem 3. *Strong induction ⇔ mathematical induction.*

Proof. If one has shown that $P(k) \rightarrow P(k+1)$, then it automatically follows that

$$[P(1) \wedge \cdots \wedge P(k)] \rightarrow P(k+1).$$

In other words, ordinary induction ⇒ strong induction.

Conversely, suppose that $P(n)$ is a statement that one can prove using strong induction. Let $Q(n)$ be $P(1) \wedge \cdots \wedge P(n)$. Clearly $\forall n, P(n)$ is logically equivalent to $\forall n, Q(n)$. We show how $\forall n, Q(n)$ can be proved using ordinary induction. First, $Q(1)$ is true because $Q(1) = P(1)$ and $P(1)$ is true by the basis step for the proof of $\forall n, P(n)$ by strong induction. Now suppose that $Q(k)$ is true, i.e., $P(1) \wedge \cdots \wedge P(k)$ is true. By the proof of $\forall n, P(n)$ by strong induction it follow that $P(k+1)$ is true. But $Q(k) \wedge P(k+1)$ is just $Q(k+1)$. Thus we have proved $\forall n, Q(n)$ by ordinary induction. □

Theorems 1, 2, and 3 above show that the well-ordering property, the principle of mathematical induction, and strong induction are all equivalent.