Unit 4
Induction and Recursion

4.1 Mathematical Induction

- To prove that P(n) is true for all positive integers n, where P (n) is a propositional function, we complete two steps:
    - *BASIS STEP:* We verify that P (1) is true.
    - *INDUCTIVE STEP:* We show that the conditional statement P (k) → P (k + 1) is true for all positive integers k.
- To complete the inductive step of a proof using the principle of mathematical induction, we assume that P(k) is true for an arbitrary positive integer k and show that under this assumption, P (k + 1) must also be true. The assumption that P (k) is true is called the *inductive hypothesis*.

EXAMPLE 1: Show that if n is a positive integer, then

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

Solution:

- Let P (n) be the proposition that the sum of the first n positive integers, 1 + 2 +⋯ n, is n(n+1)/2.
- We must do two things to prove that P (n) is true for n = 1, 2, 3,.... Namely, we must show that P(1) is true and that the conditional statement P(k) implies P(k + 1) is true for k = 1, 2, 3,....
    - BASIS STEP: P (1) is true, because $1 = \frac{1(1+1)}{2} = 1$, so basis step holds.
    - INDUCTIVE STEP: For the inductive hypothesis we assume that P (k) holds for an arbitrary positive integer k. That is, we assume that

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

- Under this assumption, it must be shown that P (k + 1) is true, namely, that

$$1 + 2 + \cdots + k + (k+1) = \frac{(k+1)[(k+1)+1]}{2} = \frac{(k+1)(k+2)}{2}$$

  is also true.

- When we add k + 1 to both sides of the equation in P (k), we obtain

$$
\begin{aligned}
1+2+\cdots+k+(k+1) &\stackrel{\text{IH}}{=} \frac{k(k+1)}{2}+(k+1) \\
&= \frac{k(k+1)+2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2}.
\end{aligned}
$$

- This last equation shows that P (k + 1) is true under the assumption that P (k) is true. This completes the inductive step.
- We have completed the basis step and the inductive step, so by mathematical induction we know that P (n) is true for all positive integers n. That is, we have proven that 1 + 2 +···+ n = n(n + 1)/2 for all positive integers n.

EXAMPLE 2: Prove by the mathematical induction that "The sum of the first n positive odd integers is n^2."

Solution:

- Let P (n) denote the proposition that the sum of the first n odd positive integers is n^2.
- To use mathematical induction to prove this conjecture, we must first complete the basis step; that is, we must show that P (1) is true.
- Then we must carry out the inductive step; that is, we must show that P (k + 1) is true when P (k) is assumed to be true.
- We now attempt to complete these two steps.
    - BASIS STEP: P (1) states that the sum of the first one odd positive integer is 1^2. This is true because the sum of the first odd positive integer is 1. The basis step is complete.
    - INDUCTIVE STEP: The inductive hypothesis is the statement that P (k) is true for an arbitrary positive integer k, that is,

$$1 + 3 + 5 +\cdots+ (2k - 1) = k^2.$$

- To show that ∀k(P (k) →P (k + 1)) is true, we must show that if P (k) is true (the inductive hypothesis), then P (k + 1) is true. Note that P (k + 1) is the statement that

$$1 + 3 + 5 +\cdots+ (2k - 1) + (2k + 1) = (k + 1)^2.$$

- So, assuming that P (k) is true, it follows that

$$
\begin{aligned}
1+3+5+\cdots+(2k-1)+(2k+1) &= [1+3+\cdots+(2k-1)]+(2k+1) \\
&\stackrel{\text{IH}}{=} k^2+(2k+1) \\
&= k^2+2k+1 \\
&= (k+1)^2.
\end{aligned}
$$

- We have now completed both the basis step and the inductive step. Hence Proved

Assignment

1. Use mathematical induction to show that $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ for all nonnegative integers n.
2. Use mathematical induction to prove this formula for the sum of a finite number of terms of a geometric progression with initial term a and common ratio r:

$$\sum_{j=0}^{n} ar^j = a + ar + ar^2 + \cdots + ar^n = \frac{ar^{n+1} - a}{r - 1} \qquad \text{when } r \neq 1,$$

   where n is a nonnegative integer.
3. Use mathematical induction to prove the inequality $n < 2^n$ for all positive integers n.
4. Use mathematical induction to prove that $2^n < n!$ for every integer n with $n \geq 4$. (Note that this inequality is false for n = 1, 2, and 3.)
5. Use mathematical induction to prove that $n^3 - n$ is divisible by 3 whenever n is a positive integer.
6. Use mathematical induction to show that if S is a finite set with n elements, where n is a nonnegative integer, then S has 2^n subsets.

4.2 Strong Induction

- To prove that P(n) is true for all positive integers n, where P (n) is a propositional function, we complete two steps:
  - *BASIS STEP:* We verify that the proposition P (1) is true.
  - *INDUCTIVE STEP:* We show that the conditional statement $[P(1) \wedge P(2) \wedge \cdots \wedge P(k)] \rightarrow P(k+1)$ is true for all positive integers k.
- Note that when we use strong induction to prove that P (n) is true for all positive integers n, our inductive hypothesis is the assumption that P(j) is true for j = 1, 2,...,k.
- That is, the inductive hypothesis includes all k statements P (1), P (2), . . . , P (k).
- Because we can use all k statements P (1), P (2), . . . , P (k) to prove P (k + 1), rather than just the statement P (k).
- Strong induction is sometimes called the second principle of mathematical induction or complete induction.

EXAMPLE 1: Show that if n is an integer greater than 1, then n can be written as the product of primes.

Solution:

- Let P (n) be the proposition that n can be written as the product of primes.
  - BASIS STEP: P (2) is true, because 2 can be written as the product of one prime, itself.
  - 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, it must be shown 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 $2 \le a \le b < k+1$.
- 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, it can be written as the product of primes, namely, those primes in the factorization of a and those in the factorization of b.

Well-Ordering Property

- Every nonempty set of nonnegative integers has a least element.
- The well-ordering property can often be used directly in proofs.

EXAMPLE 1: Use the well-ordering property to prove the division algorithm. Recall that the division algorithm states that if a is an integer and d is a positive integer, then there are unique integers q and r with $0 \le r < d$ and $a = dq + r$.

Solution: 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 $r \ge d$. Because $a = dq_0 + r$, it follows that $a - d(q_0 + 1) = (a - dq_0) - d = r - d \ge 0$.

Consequently, there are integers q and r with $0 \le r < d$. This proofs that r and q are unique.

4.3 Recursive Definitions and Structural Induction

Recursively Defined Functions

- We use two steps to define a function with the set of nonnegative integers as its domain:
  - BASIS STEP: Specify the value of the function at zero.
  - RECURSIVE STEP: Give a rule for finding its value at an integer from its values at smaller integers.
- Such a definition is called a *recursive or inductive definition*.
- Recursively defined functions are *well defined*. That is, for every positive integer, the value of the function at this integer is determined in an unambiguous way.

EXAMPLE 1: Suppose that f is defined recursively by

$f(0) = 3,$

$f(n + 1) = 2f(n) + 3.$

Find $f(1)$, $f(2)$, $f(3)$, and $f(4)$.

Solution: From the recursive definition it follows that

$f(1) = 2f(0) + 3 = 2 \cdot 3 + 3 = 9,$

$f(2) = 2f(1) + 3 = 2 \cdot 9 + 3 = 21,$

$f(3) = 2f(2) + 3 = 2 \cdot 21 + 3 = 45,$

$f(4) = 2f(3) + 3 = 2 \cdot 45 + 3 = 93.$

EXAMPLE 2: Give a recursive definition of a^n, where a is a nonzero real number and n is a nonnegative integer.

Solution:

- The recursive definition contains two parts.
- First a^0 is specified, namely, $a^0 = 1$.
- Then the rule for finding a^{n+1} from an, namely, $a^{n+1} = a \cdot a^n$, for n = 0, 1, 2, 3,..., is given.
- These two equations uniquely define a^n for all nonnegative integers n.

Assignment

1. Give a recursive definition of $\sum_{k=0}^{n} a_k$.
2. Show that whenever $n \geq 3, f_n > \alpha^{n-2}$, where $\alpha = (1 + \sqrt{5})/2$.

Recursively Defined Sets and Structures

- Recursive definitions of sets have two parts, a basis step and a recursive step.
- In the basis step, an initial collection of elements is specified.
- In the recursive step, rules for forming new elements in the set from those already known to be in the set are provided.
- Recursive definitions may also include an exclusion rule, which specifies that a recursively defined set contains nothing other than those elements specified in the basis step or generated by applications of the recursive step.

EXAMPLE: Consider the subset S of the set of integers recursively defined by

BASIS STEP: $3 \in S$.

RECURSIVE STEP: If $x \in S$ and $y \in S$, then $x + y \in S$.

The new elements found to be in S are 3 by the basis step, 3 + 3 = 6 at the first application of the recursive step, 3 + 6 = 6 + 3 = 9 and 6 + 6 = 12 at the second application of the recursive step, and so on.

Structural Induction

- Instead of using mathematical induction directly to prove results about recursively defined sets, we can use a more convenient form of induction known as structural induction.
- A proof by structural induction consists of two parts. These parts are
  - BASIS STEP: Show that the result holds for all elements specified in the basis step of the recursive definition to be in the set.
  - RECURSIVE STEP: Show that if the statement is true for each of the elements used to construct new elements in the recursive step of the definition, the result holds for these new elements.

EXAMPLE: Show that every well-formed formula for compound propositions contains an equal number of left and right parentheses.

Solution:

BASIS STEP: Each of the formula T, F, and s contains no parentheses, so clearly they contain an equal number of left and right parentheses.

RECURSIVE STEP: Assume p and q are well-formed formulae each containing an equal number of left and right parentheses. That is, if l_p and l_q are the number of left parentheses in p and q, respectively, and r_p and r_q are the number of right parentheses in p and q, respectively, then $l_p = r_p$ and $l_q = r_q$.

To complete the inductive step, we need to show that each of $(\neg p)$, $(p \vee q)$, $(p \wedge q)$, $(p \rightarrow q)$, and $(p \leftrightarrow q)$ also contains an equal number of left and right parentheses. The number of left parentheses in the first of these compound propositions equals $l_p + 1$ and in each of the other compound propositions equals $l_p + l_q + 1$. Similarly, the number of right parentheses in the first of these compound propositions equals $r_p + 1$ and in each of the other compound propositions equals $r_p + r_q + 1$. Because $l_p = r_p$ and $l_q = r_q$, it follows that each of these compound expressions contains the same number of left and right parentheses.

This completes the proof by structural induction.

Recursive Algorithms

An algorithm is called recursive if it solves a problem by reducing it to an instance of the same problem with smaller input.

EXAMPLE 1: Give a recursive algorithm for computing n!, where n is a nonnegative integer.

```
factorial(n)
{
        if(n==0)
                return 1;
        else
                return n*factorial(n-1);
}
```

Assignment

1. Give a recursive algorithm for computing a^n, where a is a nonzero real number and n is a nonnegative integer.
2. Give a recursive algorithm for computing the greatest common divisor of two nonnegative integers a and b with a<b.
3. Devise a recursive algorithm for computing $b^n \bmod m$, where b, n, and m are integers with $m \geq 2$, $n \geq 0$, and $1 \leq b < m$.
4. Express the linear search algorithm as a recursive procedure.
5. Construct a recursive version of a binary search algorithm.

Proving Recursive Algorithms Correct

Mathematical induction, and its variant strong induction, can be used to prove that a recursive algorithm is correct, that is, that it produces the desired output for all possible input values.

EXAMPLE: Prove that algorithm, "For computing a^n, where a is a nonzero real number and n is a nonnegative integer", is correct.

Solution: We use mathematical induction on the exponent n.

BASIS STEP: If n = 0, the first step of the algorithm tells us that power(a, 0) = 1. This is correct because $a^0 = 1$ for every nonzero real number a. This completes the basis step.

INDUCTIVE STEP: The inductive hypothesis is the statement that power(a, k) = a^k for all $a \neq 0$ for an arbitrary nonnegative integer k. That is, the inductive hypothesis is the statement that the algorithm correctly computes a^k. To complete the inductive step, we show that if the inductive hypothesis is true, then the algorithm correctly computes a^{k+1}. Because k + 1 is a positive integer, when the algorithm computes a^{k+1}, the algorithm sets power(a, k + 1)=a· power (a, k).

By the inductive hypothesis, we have power (a, k) = a^k, so power (a, k + 1) = a · power (a, k) = $a \cdot a^k = a^{k+1}$. This completes the inductive step.

We have completed the basis step and the inductive step, so we can conclude that above Algorithm always computes a^n correctly when $a \neq 0$ and n is a nonnegative integer.

Assignment

1. Prove that the algorithm is correct that "Devise a recursive algorithm for computing $b^n \bmod m$, where b, n, and m are integers with $m \geq 2$, $n \geq 0$, and $1 \leq b < m$."