CHAPTER 3 INDUCTION

SECTION 3.1 MATHEMATICAL INDUCTION

Mathematical induction is used to prove statements that asserts that $P(n)$ is true for all $n \in \mathbb{Z}^+$ where $P(n)$ is a propositional function. It is an extremely important proof technique.

PRINCIPLE OF MATHEMATICAL INDUCTION

To prove $\forall n \in \mathbb{Z}^+(P(n))$ where $P(n)$ is a propositional function, we complete two steps:

BASE STEP: Verify that $P(1)$ is true.

INDUCTIVE STEP: Show that $\forall k \in \mathbb{Z}^+(P(k) \to P(k+1))$ is true.

To complete the inductive step, we assume that $P(k)$ is true, (this assumption is known as the **INDUCTION HYPOTHESIS**), and prove that $P(k+1)$ is true. (It may seem circular and thus requires some clarification. We are not asserting that $P(k)$ is true for all k here. What we are saying is that under the hypothesis that $P(k)$ is true for one k, we can prove that $P(k+1)$ is true.)

What we do here is the following.

$$\begin{aligned} P(1) &\quad \text{(Base step)} \\ P(1) \Rightarrow P(2) & \\ P(2) \Rightarrow P(3) & \\ P(3) \Rightarrow P(4) & \\ \cdots & \end{aligned}$$

Eventually, we get $P(5), P(6), \ldots$.

EXAMPLE

- Prove that $\forall n \in \mathbb{Z}^+$, $\displaystyle\sum_{i=1}^{n} i = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

PROOF: Let $P(n)$ be the proposition that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Base step: P(1) is true since $\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}$.

Inductive step: Assume that $P(k)$ is true, where $k \geq 1$, i.e.,

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}.$$

Then $P(k+1)$ is true since

$$\begin{aligned}\sum_{i=1}^{k+1} i &= \Big(\sum_{i=1}^{k} i\Big) + (k+1) = \frac{k(k+1)}{2} + (k+1) \quad \text{(we use } P(k) \text{ here)}\\ &= \frac{(k+1)(k+2)}{2} = \frac{(k+1)((k+1)+1)}{2}.\end{aligned}$$

Thus $P(n)$ is true for all $n \in \mathbb{Z}^+$ by mathematical induction.

- Prove that $n < 2^n$ for all $n \in \mathbb{Z}^+$.

PROOF: Let $P(n)$ be the proposition that $n < 2^n$.

Base step: $P(1)$ is true since $1 < 2^1$.

Inductive step: Assume $P(k)$ is true. From $P(k)$, we have $k < 2^k$. Add 1 to both sides, we have

$$\begin{aligned}k+1 &< 2^k + 1\\ &< 2^k + 2^k = 2^{k+1}\end{aligned}$$

and hence $P(k+1)$ is true.

Therefore by mathematical induction $n < 2^n$ for all $n \in \mathbb{Z}^+$.

- The **HARMONIC NUMBERS** H_j, $j \in \mathbb{Z}^+$, are defined by

$$H_j = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{j}.$$

Prove that $H_{2^n} \geq 1 + \frac{n}{2}$ for all $n \in \mathbb{Z}_{\geq 0}$.

PROOF: Let $P(n)$ be the proposition that $H_{2^n} \geq 1 + \frac{n}{2}$.

Base step: $P(0)$ is true since $H_{2^0} = \frac{1}{1} \geq 1 + \frac{0}{2}$.

Inductive step: Assume that $P(0), \ldots, P(k)$ are true. Then

$$\begin{aligned}H_{2^{k+1}} &= \Big(\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{2^k}\Big) + \Big(\frac{1}{2^k+1} + \frac{1}{2^k+2} + \cdots + \frac{1}{2^{k+1}}\Big)\\ &= H_{2^k} + \Big(\frac{1}{2^k+1} + \frac{1}{2^k+2} + \cdots + \frac{1}{2^{k+1}}\Big)\\ &\geq \Big(1 + \frac{k}{2}\Big) + \Big(\frac{1}{2^k+1} + \frac{1}{2^k+2} + \cdots + \frac{1}{2^{k+1}}\Big) \quad \text{(Use } P(k) \text{ here)}\\ &\geq \Big(1 + \frac{k}{2}\Big) + \Big(\frac{1}{2^{k+1}} + \frac{1}{2^{k+1}} + \cdots + \frac{1}{2^{k+1}}\Big)\\ &= \Big(1 + \frac{k}{2}\Big) + 2^k \cdot \frac{1}{2^{k+1}} = 1 + \frac{k+1}{2}\end{aligned}$$

Thus $P(k+1)$ is true and the result follows by mathematical induction.

THEOREM: NUMBER OF SUBSETS OF A FINITE SET

A set with n elements has 2^n subsets.

PROOF: Let $Q(n)$ be the above proposition.

Base step: When $n = 0$, the set concerned is $\emptyset$ which has only one subset. Thus $Q(0)$ is true.

Inductive step: Assume that $Q(k)$ is true.

Let X be any set with $k+1$ elements. Take a particular element $a \in X$. Then $Y = X - \{a\}$ is a set with k elements. By the induction hypothesis,

$$|P(Y)| = 2^k.$$

Subsets of X can be divided into two types:

(i) Those that do not contain a. These are precisely the subsets of Y and there are 2^k subsets of this type.

(ii) Those that contain a. If the element a is deleted, they become subsets of Y. Thus each corresponds to a subset of Y. Therefore there are also 2^k subsets of this type.

Thus

$$|P(X)| = 2^k + 2^k = 2^{k+1}.$$

Hence $Q(k+1)$ is true.

The result then follows by the principle of mathematical induction.

SUM OF GP

For all integers $n \in \mathbb{Z}_{\geq 0}$, and all real numbers $r \neq 1$:

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}.$$

PROOF: When $n = 0$, l.h.s $= 1$ and r.h.s $= \frac{r-1}{r-1} = 1$. Thus the formula is true when $n = 0$.

Assume that the formula is true for $n = k$. Thus $\sum_{i=0}^{k} r^i = \frac{r^{k+1}-1}{r-1}$. Then

$$\sum_{i=0}^{k+1} r^i = \sum_{i=0}^{k} r^i + r^{k+1} = \frac{r^{k+1} - 1}{r - 1} + r^{k+1} = \frac{r^{k+2} - 1}{r - 1}.$$

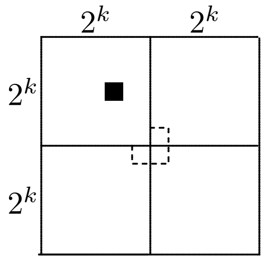
Thus the formula is also true at $k + 1$.

By the principle of mathematical, the formula is true.

- Prove that for any integer $n \geq 1$, if one square is removed from a $2^n \times 2^n$ checkerboard, the remaining squares can be covered by an L-tromino. (An L-tromino is an L-shape formed by 3 squares of the checkerboard.)

PROOF: Let $P(n)$ be the given statement.

Base step. $P(1)$ is true since the board is itself an L-tromino.



Assume that $P(k)$ is true. Consider a $2^{k+1} \times 2^{k+1}$ checkerboard with one square removed. Divide the checkerboard in 4 equal quadrants so that each quadrant is a $2^k \times 2^k$ board. Without loss of generality, assume that the removed square is from the first quadrant. Now remove a tromino from the centre of the board. (This tromino has one square in each of the last three quadrants.) Now we are left with four $2^k \times 2^k$ checkerboards, each with a square removed. Thus by the induction hypothesis, each can be covered by trominoes. Hence the $2^{k+1} \times 2^{k+1}$ checkerboard with one square removed can be so covered as well. The proof is now complete by mathematical induction.

SECTION 3.2 STRONG MATHEMATICAL INDUCTION

STRONG MATHEMATICAL INDUCTION

To prove $\forall n \in \mathbb{Z}^+(P(n))$ where $P(n)$ is a propositional function, we complete two steps:

BASE STEP: Verify that $P(1), ..., P(m)$ are all true. (i.e. for the first few values of n, $P(n)$ is true.)

INDUCTIVE STEP: Show that $\forall k \geq m(P(1) \wedge P(2) \wedge \cdots \wedge P(k) \rightarrow P(k+1))$ is true.

To complete the inductive step, we assume that $P(1), \ldots, P(k)$ are true, (this assumption is known as the **INDUCTION HYPOTHESIS**), and prove that $P(k+1)$ is true. (It may seem circular and thus requires some clarification. We are not asserting that $P(k)$ is true for all k here. What we are saying is that under the hypothesis that $P(1), \ldots, P(k)$ are true, we can prove that $P(k+1)$ is true.)

What we do here is the following.

$$\begin{aligned} P(1), P(2) & \quad \text{(Base step when } m=2) \\ P(1) \wedge P(2) \Rightarrow P(3) & \\ P(1) \wedge P(2) \wedge P(3) \Rightarrow P(4) & \\ \cdots & \end{aligned}$$

Eventually, we get $P(5), P(6), \ldots$.

REMARK

Difference between proving by normal induction and by strong induction:

- For normal induction, only $P(k)$ is assumed when proving $P(k+1)$.
- For strong induction, we may assume $P(1), \ldots, P(k)$ when proving $P(k+1)$.
- Usually proving by strong induction is easier, since we can assume more information when trying to prove $P(k+1)$ in the inductive step.

EXAMPLE

- Suppose that $h_0, h_1, \ldots$ is a sequence defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3 \qquad \text{and} \qquad h_k = h_{k-1} + h_{k-2} + h_{k-3} \quad \text{for} \quad k \geq 3$$

Prove that $h_n \leq 3^n$ for all $n \geq 0$.

PROOF: Let $P(n)$ be the proposition that $h_n \leq 3^n$.

Base step: Note that $h_n \leq 3^n$ for $n = 0, 1, 2$.

Inductive step: Now assume that it's true for all $n = 0, 1, 2, \dots k$, where $k \geq 2$. Then

$$h_{k+1} = h_k + h_{k-1} + h_{k-2} \leq 3^k + 3^{k-1} + 3^{k-2} \leq 3 \times 3^k = 3^{k+1}.$$

Hence the result holds for $n = k+1$ and the proof is complete.

DEFINITION:

FIBONACCI NUMBERS $F_0, F_1, \dots$ are defined by

$$F_0 = 0, F_1 = 1$$
$$F_{n+1} = F_n + F_{n-1} \quad \text{for } n \geq 1$$

$F_0 = 0,\ F_1 = 1,\ F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 5, \dots$

• Prove that for $n \geq 3$, $F_n > \alpha^{n-2}$, where $\alpha = (1+\sqrt{5})/2$.

PROOF: Let $P(n)$ be $F_n > \alpha^{n-2}$, $n \geq 3$.

Base step: Since $F_3 = 2 > \alpha$, and $F_4 = 3 \geq \alpha^2$, $P(3)$ and $P(4)$ are true.

We need both as $P(3)$ on its own will not yield $P(4)$.

Inductive step:

Suppose $P(n)$ is true, i.e., $F_n > \alpha^{n-2}$ for $n = 3, \dots, k$. First note that

$$\alpha^2 = \frac{(1+\sqrt{5})^2}{4} = \frac{3+\sqrt{5}}{2} = 1 + \alpha.$$

Now $P(k+1)$ is true since

$$F_{k+1} = F_k + F_{k-1} > \alpha^{k-2} + \alpha^{k-3} = \alpha^{k-3}(\alpha + 1) = \alpha^{k-1}$$

THEOREM: (Well-Ordering Principle)

Every nonempty subset of $\mathbb{Z}_{\geq 0}$ has a least element.

REMARK

• The least element is the smallest element in the set.

• The least element in the set $\{3, 4, 5, 6, 10\}$ is 3

• The set $(0, 1)$ does not have a least element. For if $a \in (0, 1)$ is a least element, then $a/2 \in (0, 1)$ and is $< a$. This gives a contradiction.

PROOF:

The theorem says

$$\forall X \subseteq \mathbb{Z}_{\geq 0}, \quad X \text{ is non-empty} \Rightarrow X \text{ has a least element.}$$

Its contrapositive is

$$\forall X \subseteq \mathbb{Z}_{\geq 0}, \quad X \text{ has no least element} \Rightarrow X \text{ is empty.}$$

Assume $X \subseteq \mathbb{Z}_{\geq 0}$ has no least element. We want to prove that $\forall n \in \mathbb{Z}^+, n \notin X$.

Let $P(n)$ be $n \notin X$.

Base step: $0 \notin X$. Otherwise, 0 would be the least element of X, contradicting the assumption "X has no least element". Therefore, $P(0)$ is true.

Inductive step: Suppose $P(0), \ldots, P(k)$ are all true. That is, $j \notin X$ for all $j = 0, ..., k$.

Then we must have $k + 1 \notin X$. Otherwise, $k + 1$ would be the least element of X, contradicting the assumption "X has no least element". Therefore, $P(k + 1)$ is true.

By strong mathematical induction, $\forall n, P(n)$ (i.e. $\forall n, n \notin X$). Hence, X is empty.

SECTION 3.3 RECURSIVELY DEFINED SEQUENCES

Consider the following sequences:

- $2,\ 9,\ 16,\ 23,\ 30,\ldots$
- $1,\ 2,\ 4,\ 8,\ 16,\ldots$
- $2,\ 3,\ 6,\ 18,\ 108,\ldots$

Observe that if the sequence is denoted $a_1, a_2, a_3, \ldots$, then three sequences above satisfies:

- $a_{n+1} = a_n + 7$ for all $n \in \mathbb{Z}^+$;
- $a_{n+1} = 2a_n$ for all $n \in \mathbb{Z}^+$;
- $a_{n+1} = a_n \times a_{n-1}$ for all $n \in \mathbb{Z}_{\geq 2}$.

These are **recursively defined** sequences, where, other than the first few terms, each successive term depends on the previous terms in such a sequence.

EXAMPLE

- The Fibonacci sequence $F_0, F_1, F_2, F_3, \ldots$ is defined recursively.

Sets can also be defined recursively.

EXAMPLE

- The set E of all positive even integers can be defined recursively as follows.

  Base step $2 \in E$.

  Recursive step If $x \in E$, then $x + 2 \in E$.

- Consider the subset $S \subseteq \mathbb{Z}^+$ defined by

  Base step $3 \in S$.

  Recursive step If $x \in S$ and $y \in S$, then $x + y \in S$.

The first recursive step yields $3 + 3 = 6 \in S$ by taking $x = y = 3$. The next step yields $3+6 = 9 \in S$ and $6+6 = 12 \in S$. We shall prove that S consists of all multiples of 3. Let A be the set of multiples of 3. We want to prove that $A = S$.

First we prove that $A \subseteq S$ by induction. Let $P(n)$ be "$3n \in S$". Since A consists of integers of the form $3n$, we need to prove that $P(n)$ is true for all n. The Base step is trivial. for the inductive step, we assume that $P(k)$ is true, i.e., $3k \in S$. Then $3(k + 1) = 3k + 3 \in S$ since $3k \in S$ and $3 \in S$. Thus $P(k + 1)$ is true as well.

Next we need to prove that $S \subseteq A$. For this we need to show that all the integers generated recursively are multiples of 3. Since 3 is clearly a multiple of 3, the Base step gives a number which is a multiple of 3. Next, we need to show that the recursive step also generates multiples of 3. Thus we need to show that $x + y$ is a multiple of 3 given that $x, y \in S$ and are also multiples of 3. This is true since x and y being multiply of 3 implies that $x + y$ is a multiple of 3.

Existence and Uniqueness of Recursively defined Sequences

THEOREM:

Let $m \in \mathbb{Z}^+$, $a_0, a_1, \ldots, a_{m-1} \in A$ and $f : A^m \to A$ be a function. Then there is a unique infinite sequence $x_0, x_1, \ldots$ defined by

BASE STEP $x_0 = a_0, x_1 = a_1, \ldots x_{m-1} = a_{m-1}$

INDUCTIVE STEP $x_n = f(x_{n-1}, x_{n-2}, \ldots, x_{n-m})$, for all $n \geq m$.

PROOF:

EXISTENCE Proof by contradiction. Suppose there is no infinite sequence $x_0, x_1, \ldots$ defined by recursion. Then the sequence must stop somewhere. That is, the set

$$S_1 = \{n \in \mathbb{Z}_{\geq 0} \mid \quad x_n \text{ is not defined} \quad \}$$

is non-empty. Then S_1 must have the **least element**, say n_1, by the well-ordering property. Then x_{n_1} is not defined.

$n_1 \neq 0, \ldots m-1$, because $x_0 = a_0, x_1 = a_1, \ldots x_{m-1} = a_{m-1}$ are defined in the base step. Therefore, $n_1 \geq m$.

But then x_{n_1} could be defined by $x_{n_1} = f(x_{n_1-1}, x_{n_1-2}, \ldots, x_{n_1-m})$ contradicting "x_{n_1} is not defined". Why?

- Note that $n_1 - 1, n_1 - 2, \ldots, n_1 - m$ are not in S_1, because n_1 is the **least element** of S_1.
- $x_{n_1-1}, x_{n_1-2}, \ldots, x_{n_1-m}$ are defined
- Then $f(x_{n_1-1}, x_{n_1-2}, \ldots, x_{n_1-m})$ is defined.

UNIQUENESS Similar proof as EXISTENCE.

Proof by contradiction. Suppose there are two different infinite sequences $x_0, x_1, \ldots$ and $y_0, y_1, \ldots$ defined by recursion. Then these two sequences must be different somewhere. That is, the set

$$S_2 = \{n \in \mathbb{Z}_{\geq 0} \mid x_n \neq y_n\}$$

is non-empty. Then S_2 must have the **least element**, say n_2, by the well-ordering property. Then $x_{n_2} \neq y_{n_2}$.

$n_2 \neq 0, \ldots m-1$, because $x_0 = y_0 = a_0, x_1 = y_1 = a_1, \ldots x_{m-1} = y_{m-1} = a_{m-1}$ are defined in the base step. Therefore, $n_2 \geq m$.

But then $x_{n_2} = y_{n_2} = f(x_{n_2-1}, x_{n_2-2}, \ldots, x_{n_2-m})$ contradicting "$x_{n_2} \neq y_{n_2}$. Why?

- Note that $n_2 - 1, n_2 - 2, \ldots, n_2 - m$ are not in S_2, because n_2 is the **least element** of S_2.
- Then $(x_{n_2-1}, x_{n_2-2}, \ldots, x_{n_2-m}) = (y_{n_2-1}, y_{n_2-2}, \ldots, y_{n_2-m})$.
- Then $x_{n_2} = f(x_{n_2-1}, x_{n_2-2}, \ldots, x_{n_2-m}) = f(y_{n_2-1}, y_{n_2-2}, \ldots, y_{n_2-m}) = y_{n_2}$.