Induction

- Principle of Mathematical Induction
- Proofs by Induction
- Strong Induction
- Well Ordering Principle

Imdad ullah Khan

Strong Induction

Principle of Mathematical Induction

$$\left[\,P(0) \wedge \forall k \geq 0 \left[P(k) \rightarrow P(k+1)\right]\,\right] \longrightarrow \forall n \geq 0\, P(n)$$

Proof using Induction

- *Basis Step:* Prove $P(0)$ is true
- *IH:* Assume $P(n)$
- *Inductive Step:* Using $P(n)$, prove $P(n+1)$

Principle of Strong Mathematical Induction

$$\left[\,P(0) \wedge \forall k \geq 0 \left[\forall\, 0 \leq i \leq k\;\, P(i) \rightarrow P(k+1)\right]\,\right] \longrightarrow \forall n \geq 0\, P(n)$$

Proof using Strong Induction

- *Basis Step:* Prove $P(0)$ is true
- *IH:* Assume $P(k)$ is true for all $1 \leq k \leq n$
- *IS:* Using $\forall\; k \leq n\; P(k)$, prove $P(n+1)$

Well Ordering Principle

Principle of Well Ordering

Any nonempty set of nonnegative integers has a smallest element

What is the smallest element of

ICP 10-11 $\left\{x \in \mathbb{Z} : x < 7\right\}$

ICP 10-12 $\left\{x \in \mathbb{R} : 0 < x < 1\right\}$

ICP 10-13 $\left\{3.9 + \frac{1}{n} : n \in \mathbb{Z}^+\right\}$

ICP 10-14 $\left\{ \left\lfloor 3.9 + \frac{1}{n} \right\rfloor : n \in \mathbb{Z}^+\right\}$

Why induction work

Principle of Well Ordering

Any nonempty set of nonnegative integers has a smallest element

Principle of Mathematical Induction

$$\Big[\, P(0) \wedge \forall k \geq 0 \,\big[P(k) \rightarrow P(k+1)\big] \,\Big] \longrightarrow \forall n \geq 0\, P(n)$$

Proof using Mathematical Induction

1. *Basis Step:* Prove $P(0)$ is true
2. *Inductive Step:* $\underbrace{\text{Assume } P(n)}_{\text{IH:}}$ Using $P(n)$, prove $P(n+1)$

We argue why induction make sense using the principle of well ordering and how they are essentially equivalent

Why induction work

$$[\underbrace{P(0)}_{\text{basis step}} \wedge \underbrace{\forall k\,(P(k) \to P(k+1))}_{\text{induction step}}] \longrightarrow \forall n \geq 0\; P(n)$$

Suppose we proved 1) $P(0)$ and 2) $\forall k\; P(k) \to P(k+1)$

and assume $\neg\forall n\; P(n) \equiv \exists n\; \neg P(n)$ ▷ i.e. induction does not work

Let $S = \{\, k : \neg P(k) \,\}$ ▷ $S \neq \emptyset$, why?

Let m be its least element ▷ one exists by well-ordering

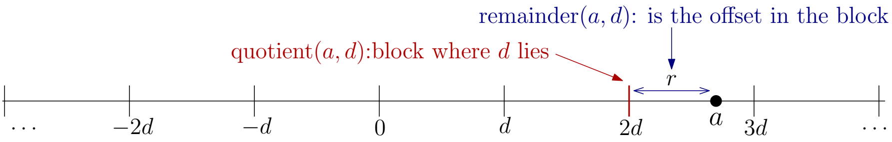
- $P(m)$ is false $\because m \in S$
  - $m \neq 0 \because P(0)$ is true by 1)
  - $P(m-1)$ is true $\because m$ is the least element of S
- But $\underbrace{P(m-1)}_{\text{true}} \to \underbrace{P(m)}_{\text{false}}$ is true by 2) ▷ Contradiction

Proof using Principle of Well Ordering

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 $a = dq + r$

- q is called the quotient
- r is called the remainder
- d is called the divisor
- a is called the dividend



Proof using Principle of Well Ordering

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 $a = dq + r$

quotient and remainder when 11 is divided by 5

$$11 = 5 \times 2 + 1$$

Notation:

$q = 2 = 11 \text{ div } 5$
$r = 1 = 11 \bmod 5$

Proof using Principle of Well Ordering

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 $a = dq + r$

quotient and remainder when -11 is divided by 5

$$-11 \ = \ 5 \times -3 + 4$$

Notation:

$q = -3 \ = \ -11 \ \text{div} \ 5$
$r = 4 \ = \ -11 \ \text{mod} \ 5$

Proof using Principle of Well Ordering

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 $a = dq + r$

$11 \ = \ 5 \times 2 + 1$

Given positive a, repeatedly subtract d until what remains r is $0 \leq r < d$

$-11 \ = \ 5 \times -3 + 4$

Given negative a, repeatedly add d until what remains r is $0 \leq r < d$

Proof using Principle of Well Ordering

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 $a = dq + r$

Existence: $S = \{a - dq \geq 0 : q \in \mathbb{Z}\}$ $\quad S \neq \emptyset$

Let $r = a - dq_0$ be the least element of S $\quad r \geq 0$

$r < d$?

If $r \geq d$, then $a - d(q_0 + 1) = r - d \geq 0$

$r - d < r$ is in S, $\quad \triangleright$ a contradiction to minimality of r

There are q and $0 \leq r < d$ with $a = dq + r$

Proof using Principle of Well Ordering

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 $a = dq + r$

Uniqueness:

Let $a = dq_1 + r_1$ and $a = dq_2 + r_2$ with $q_1 \neq q_2$ and $0 \leq r_1 \neq r_2 < d$

$$\underbrace{dq_1 + r_1}_{a} - \underbrace{dq_2 + r_2}_{a} = 0 \implies d(q_1 - q_2) = r_2 - r_1$$

This means d divides $(r_2 - r_1) \implies$ either $\begin{cases} r_2 = r_1 \\ d \leq |(r_2 - r_1)| \end{cases}$ or

$$[0 \leq r_1 \neq r_2 < d] \implies -d < r_2 - r_1 < d \implies |r_2 - r_1| < d$$

$$\implies r_1 = r_2$$

From $r_1 = r_2$, we also get $q_1 = q_2$