CSC236H
Introduction to the Theory of Computation

Bahar Aameri

Fall 2019 – Week 1

- A predicate is defined over some variables and denotes a statement about a set of elements.

  $n \in \mathbb{N}$

  - $O(n)$: n is an odd natural number.

  $a, b \in \mathbb{Z}$

  - $D(a, b)$: a divides b.
  - $F(Tom, Bob)$: Tom is the father of Bob.

Suppose we want to prove that a predicate P holds for all natural numbers greater than or equal to $b \in \mathbb{N}$.

That is: for all $n \in \mathbb{N}$, if $n \geq b$, then $P(n)$ holds.

Proof by Simple Induction

1. **Base Case**: Prove $P(b)$. ①

IS

2. **Induction Step**: IH
   - Let $k \in \mathbb{N}$, $k \geq b$. Assume $P(k)$ holds. (Induction Hypothesis)
   - Use the **Induction Hypothesis** to prove that $P(k+1)$ holds.
3. Use the **Principle of Simple Induction (PSI)** to conclude that for all $n \in \mathbb{N}$, if $n \geq b$, then $P(n)$ holds.

for all $n \in \mathbb{N}$, $n \geq b$, $P(n)$

PSI: If $P(b)$ holds,
and for **all** $k \in \mathbb{N}, k \geq b$, $P(k)$ implies $P(k+1)$,
then for all $n \in \mathbb{N}, n \geq b, P(n)$ holds.

$$\left[P(b) \wedge \left(\forall k \in \mathbb{N}, k \geq b \Rightarrow \left(P(k) \Rightarrow P(k+1) \right) \right) \right] \Rightarrow \forall n \in \mathbb{N}, n \geq b \Rightarrow P(n)$$

Informal Justification: Base Case (B.C.)

IS

Suppose we proved that $P(b)$ is true.
Suppose we also proved that for all $k \in \mathbb{N}$, $k \geq b$, if $P(k)$ holds then $P(k+1)$ holds.

B.C.

$$P(b) \overset{IS}{\Longrightarrow} P(b+1) \overset{IS}{\Longrightarrow} P(b+2) \overset{IS}{\Longrightarrow} P(b+3) \overset{IS}{\Longrightarrow} \ldots$$

Simple Induction – Example

Prove that for all $n \in \mathbb{N}$, $\boxed{\sum_{i=0}^{n} i = \frac{n(n+1)}{2}}$.

$$P(n): \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

WTP: for all $n \in \mathbb{N}$, $P(n)$.

B.C.: Let $k=0$.

Then $\sum_{i=0}^{0} i = 0$. Also $\frac{k(k+1)}{2} = \frac{0 \times 1}{2} = 0$. So $\sum_{i=0}^{k} i = \frac{k(k+1)}{2}$.

So $P(k)$ holds.

Let $k \in \mathbb{N}$. Assume $P(k)$ holds. [IH]

that is, $\sum_{i=0}^{k} i = \frac{k(k+1)}{2}$

IS:

WTP: $P(k+1)$ holds, that is,

$$\sum_{i=0}^{k+1} i = \frac{(k+1)(k+2)}{2}$$

$$\sum_{i=0}^{k+1} i = \sum_{i=0}^{k} i + (k+1)$$

$$= \frac{k(k+1)}{2} + (k+1) \qquad \text{\# by IH}$$

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

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

So By PSI, for all $n \in \mathbb{N}$, $P(n)$ holds.

Summary of Steps in Proof by Simple Induction

- Step 1: Define the predicate.
- Step 2: Prove the predicate holds for the **Base Case(s)** (there could be more than one base case).
- Step 3: Set up the **Induction Step (IS)**, indicate **Induction Hypothesis (IH)**, indicate **What to Prove (WTP)**.
- Step 4: Using **IH**, prove that $P(k+1)$ holds (make sure to explicitly indicate where you use IH).

Let $a_0, a_1, a_2, \ldots$ be a sequence of natural numbers such that:

- $a_0 = 1$;
- for all $n \geq 1$, $a_n = 2a_{n-1} + 1$.

$a_1 = 2a_0 + 1 = 2 \times 1 + 1 = 3$

$a_{k+1} = 2a_{k+1-1} + 1 = 2a_k + 1$

Prove that for all $n \in \mathbb{N}$, $\boxed{a_n = 2^{n+1} - 1}$.

$P(n): a_n = 2^{n+1} - 1$

WTP: for all $n \in \mathbb{N}$, $P(n)$ holds.

B.C.: Let $k = 0$

Then, $a_k = a_0 = 1$, by def.

$2^{k+1} - 1 = 2^{0+1} - 1 = 1$

$\Rightarrow a_k = 2^{k+1} - 1$, so $P(k)$ holds.

Let $k \in \mathbb{N}$. Assume $P(k)$ holds, that is

$$a_k = 2^{k+1} - 1. \quad [IH]$$

.   :

IS:

WTP: $P(k+1)$ holds, that is, $\underbrace{a_{k+1} = 2^{k+2} - 1}$

$$a_{k+1} = 2\boxed{a_k} + 1 \qquad \text{\# by def}$$

$$= 2 \times (2^{k+1} - 1) + 1 \qquad \text{\# by IH}$$

$$= 2 \times 2^{k+1} - 2 + 1$$

$$= \underbrace{2^{k+2} - 1}$$

So $P(k+1)$ holds.

Then, by PSI, for all $n \in \mathbb{N}$, $P(n)$ holds.

Prove that for all natural numbers $n > 4$, $2^n > n^2$.

$P(n): 2^n > n^2$

WTP: for all $n \in \mathbb{N}$, if $n > 4$, then $P(n)$ holds.

Base case: Let $k = 5$

$$\left.\begin{array}{l} 2^k = 2^5 = 32 \\ k^2 = 5^2 = 25 \end{array}\right\} \Rightarrow 2^k > k^2 \Rightarrow P(k) \text{ holds.}$$

Let $k \in \mathbb{N}$, $k \geq 5$. Assume $P(k)$ holds. [IH]

IS: WTP: $P(k+1)$ holds. That is, $2^{k+1} > (k+1)^2$

$$\boxed{(k+1)^2 = k^2 + 2k + 1}$$

$$2^{k+1} = 2 \times 2^k$$

$$= \underbrace{2^k}_{} + \underbrace{2^k}_{}$$

$$> \underbrace{k^2}_{} + \underbrace{k^2}_{}$$ # by IH

$$\geq k^2 + 5k$$ # Since $k \geq 5$, so $k^2 \geq 5k$

$$> k^2 + 2k + 1$$ # since $5k = 2k + 3k > 2k + 1$ as $k \geq 5$ and so $3k > 1$

$= (k+1)^2$

So $P(k+1)$ holds.

By PSI, for all $n \in \mathbb{N}$, $n \geq 5$, $P(n)$ holds.

Is it always convenient to use simple induction?

Simple Induction:

- **Induction Step**: Let $k \in \mathbb{N}, k \geq b$. Assume $P(k)$ holds. **[IH]**
  WTP: $P(k+1)$.

Example: Prove that any natural number $n \geq 2$ has a prime factorization.

$n = r_1 \times r_2 \times \dots \times r_s$ s.t. $r_1, r_2, \dots, r_s$ are prime numbers

$n = a \times b$ and $a, b \in \mathbb{N}$ and $2 \leq a, b < n$

a and b may not equal to $n-1$.

we want to have $P(a)$ and $P(b)$ as assumptions

IH for simple induction: Assume $P(k)$

IH for complete induction: Assume $P(b), P(b+1), P(b+2), \ldots$
$P(k-1), P(k)$

Proof by Complete Induction

1. **Base Case**: Prove $P(b)$.

2. **Induction Step**:

   - Let $k \in \mathbb{N}$, $k \geq b$. Assume $\boxed{P(b), P(b+1), P(b+2) \ldots, P(k)}$ hold. **[IH]**
   - Use the **Induction Hypothesis** to prove that $P(k+1)$ holds.

Complete Induction

- **Induction Step**:
  Let $k \in \mathbb{N}$, $k \geq b$. Assume $\underbrace{P(b), P(b+1), P(b+2), \ldots, P(k)}_{j}$ hold. **[IH]**

Shorter version of IH:

- **Induction Step**:
  Let $k \in \mathbb{N}$, $k \geq b$. Assume for all $j \in \mathbb{N}$, $\boxed{b \leq j \leq k}$, $P(j)$. **[IH]**

Prove that any natural number $n \geq 2$ has a prime factorization.

$P(n)$: there exist $r_1, \ldots, r_s$ s.t. $n = r_1 \times \ldots \times r_s$ and $r_1, \ldots, r_s$ are primes.

WTP: for all $n \in \mathbb{N}$, if $n \geq 2$, then $P(n)$ holds.

B.C.: Let $k = 2$.
Then $P(k)$ holds b.c. k is a prime.

Let $k \in \mathbb{N}$, $k \geq 2$. Assume for all $j \in \mathbb{N}$, $\boxed{2 \leq j < k}$, $P(j)$ holds.
[IH]

IS:

WTP: $P(k+1)$ holds.

Case 1: Assume $k+1$ is prime.

Then $k+1$ has a prime factorization and so $P(k+1)$ holds.

Case 2: Assume $k+1$ is not prime.

Then, by def, there exist $\underbrace{2 \leq}\, a, b \underbrace{<}\, k+1$, $a, b \in \mathbb{N}$, s.t. $\underline{k+1 = a \times b}$.

Then, by IH, $P(a)$ and $P(b)$ holds, meaning that there exist $t_1, \ldots, t_q$ and $s_1, \ldots, s_l$

s.t. $a = t_1 \times \dots \times t_q$ and $b = s_1 \times \dots \times s_L$ and

$t_1, \dots, t_q, s_1, \dots, s_L$ are primes

Then $\underbrace{k+1 = t_1 \times \dots \times t_q \times s_1 \times \dots \times s_L}$, that is $k+1$

has a prime factorization, and so

$P(k+1)$ holds.

By PCI, for all $n \in \mathbb{N}$, $n \geq 2$, $P(n)$ holds.

Summary of steps in proof by induction

- Step 1: Define the predicate.
- Step 2: Prove the predicate holds for all **Base Case(s)** $b_1, b_2, ..., b_t$.
- Step 3: Set up the **Induction Step (IS)**, indicate **Induction Hypothesis (IH)**, indicate **What to Prove (WTP)**.
  - Simple Induction:
    Let $k \in \mathbb{N}$, and $k \geq b_t$. Assume $P(k)$ holds. **[IH]**
    WTP: $P(k+1)$
  - Complete Induction:
    Let $k \in \mathbb{N}$, $k \geq b_t$. Assume for all $j \in \mathbb{N}$, $b_1 \leq j \leq k$, $P(j)$. **[IH]**
    WTP: $P(k+1)$
- Step 4: Using **IH**, prove that $P(k+1)$ holds (make sure to explicitly indicate where you use IH).

Summary of steps in proof by induction

Let $f_1, f_2, \ldots$ be a sequence of natural numbers which is defined as follows:

$$\begin{cases} f_n = 1, & 1 \leq n \leq 2 \\ f_n = f_{n-1} + f_{n-2}, & n \geq 3. \end{cases}$$

Consider the following sequence of natural numbers:

$$\begin{cases} a_n = 1, & 1 \leq n \leq 2 \\ a_n = a_{n-1} + a_{n-2} + 1, & \text{for } n \geq 3. \end{cases}$$

Prove that for all $n \geq 1$, $a_n = 2f_n - 1$.

$P(n)$: $a_n = 2f_n - 1$

WTP: for all $n \in \mathbb{N}$, if $n \geq 1$, then $P(n)$ holds.

B.C.1: Let $k=1$.

Then $a_k = a_1 = 1$, by def.
$2f_k - 1 = 2 \times 1 - 1 = 1$, by def
$\Rightarrow P(k)$ holds.

B.C.2: Let $k=2$.

$f_k = f_2 = 1 \Rightarrow 2f_k - 1 = 1$
$a_k = a_2 = 1$
$\Rightarrow P(k)$ holds.

Let $k \in \mathbb{N}$, $k \geq \cancel{1}\,2$. Assume for all $j \in \mathbb{N}$, $\underbrace{1 \leq j \leq k}_{[IH]}$, $P(j)$ holds.

IS: WTP: $P(k+1)$ holds. i.e., $a_{k+1} = 2f_{k+1} - 1$

$$a_{k+1} = a_k + a_{k-1} + 1 \qquad \text{\# by def of } a_{k+1}$$

$$= (2f_k - 1) + (2f_{k-1} - 1) + 1 \qquad \text{\# by IH, } P(k) \text{ and}$$

$P(k-1)$ holds since $1 \leq k \leq k$ and $\boxed{1 \leq k-1} \leq k$

since we assumed $k \geq 2$

$$= 2(f_k + f_{k-1}) - 1$$

$$= 2f_{k+1} - 1 \qquad \text{\# by def of } f_{k+1}$$

So $P(k+1)$ holds.

•   :

Example: Find the flaw with the following "proof":

Claim: For all natural numbers n, and all non-zero real numbers a, $a^n = 1$.

$P(k) : a^k = 1$.

$n=0$

Base Case: $a^0 = 1$ is true, by the definition of a^0.

another base case is needed in which $k=1$. But it's impossible to prove this base case as $P(1)$ does not hold.

Induction Step: $k \geq 1$

Let $k \in \mathbb{N}$, $k \geq 0$. Assume for all $j \in \mathbb{N}$, $0 \leq j \leq k$, $a^j = 1$. **[IH]**

$$
\begin{aligned}
a^{k+1} &= a^{(k+k)-(k-1)} && \text{\# Algebra} \\
&= \frac{a^k \cdot a^k}{a^{k-1}} && \text{\# Algebra} \\
&= \frac{1 \cdot 1}{1} && \text{\# By IH, since } \boxed{k-1},\ k \leq k \\
&= 1
\end{aligned}
$$

$k-1 \geq -1$

to apply IH for $k-1$, we must ensure that $k-1 \geq 0$, meaning that $k \geq 1$ must hold.

Something to think about (optional!)

- Is it possible to use induction to prove statements about members of the following sets? If yes, how? If no, why?
  - The set of even natural numbers.
  - The set of integer numbers $\mathbb{Z}$.
  - The set of rational numbers $\mathbb{Q}$.