MAT236 - Intro to the Theory of Computation

Callum Cassidy-Nolan

September 13, 2019

Contents

List of Definitions

List of Theorems

Chapter 1

Lecture 1

Definition 1 (Predicate)
defined over some variable and denoted by a statement about a set of elements.

Example
$$P(n) : \text{``}n \text{ is an odd natural number ''}, \text{ where } n \in \mathbb{N}$$

1.1 Simple Induction

Allows us to prove a predicate P holds for all natural numbers greater than or equal to $b \in \mathbb{N}$ that is
$$\forall n \in \mathbb{N}, n \geq b \implies P(n)$$

The principle behind it is this

- If $P(b)$ holds , and we have $\forall k \in \mathbb{N}, k \geq b, P(k) \implies P(k+1)$

- Then $\forall n \in \mathbb{N}, n \geq b \implies P(n)$ holds

Justification, Informal

- suppose $P(b)$ hold (base case)

- suppose $\forall k \in \mathbb{N}, k \geq b, P(k) \implies P(k+1)$ (Induction Step)

Then
$$P(b) \implies P(b+1) \implies \dots$$

Prove the following
$$\forall n \in \mathbb{N}, \sum_{i=0}^{n} = \frac{n(n+1)}{2}$$

Proof.
We define the following predicate

$$P(n) : \text{``} \sum_{i=0}^{n} i = \frac{n(n+1)}{2} \text{''}, \text{ where } n \in \mathbb{N}$$

■

Proof.
Be begin

- **Base Case:**
  We show that $P(0)$ holds, we know

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

  therefore right hand side equals left hand side, so we have $P(0)$ holds .

- **Induction Step:**
  Let $k \in \mathbb{N}$ and assume that $P(k)$ holds, that is

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

  We'll show that $P(k+1)$ holds, so we must show that

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

  Intuition: We need to get to our IH, let's break the summation down, we know

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

Thus by the principle of induction we have proven the original statement.   ■

Summary

1. Define the predicate

2. Prove that the base case holds

3. Induction Step: Assume the Induction Hypothesis, show what we will prove.

4. Use Induction Hypothesis to prove $P(k+1)$

We will prove

$$a_n = 2^{n+1} - 1$$

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

Proof.
We define the following predicate

$$P(n) : \text{``}a_n = 2^{n+1} - 1\text{''}, \text{ where } n \in \mathbb{N}$$

- **Base Case:**
  We show that $P(0)$ holds, we know

  $$a_0 = 2^1 - 1$$

  therefore $P(0)$ holds

- **Induction Step:**
  Let $k \in \mathbb{N}$ and assume that $P(k)$ holds, that is

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

  We'll show that $P(k+1)$ holds, so we must show that

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

  Intuition: we use the recurvie definition to access the Induction Hypothesis, we know

  $$
  \begin{aligned}
  a_{k+1} &= 2a_k + 1 \\
  &= 2\left(2^{k+1} - 1\right) + 1 \\
  &= 2^{k+2} - 2 + 1 \\
  &= 2^{k+2} - 1
  \end{aligned}
  $$

Thus by the principle of induction we have proven the original statement. ∎

Homework Quesiton   We will prove

$$\forall n \in \mathbb{N}, n > 4 \implies 2^n > n^2$$

Proof.
We define the following predicate

$$P(n) : \text{``}2^n > n^2\text{''}, \text{ where } n \in \mathbb{N}$$

- **Base Case:**
  We show that $P(5)$ holds, we know

  $$2^5 > 5^2 \Leftrightarrow 32 > 25$$

  therefore $P(5)$ holds .

- **Induction Step:**
  Let $k \in \mathbb{N}$ and assume that $P(k)$ holds, that is

  $$2^k > k^2$$

  We'll show that $P(k+1)$ holds, so we must show that

  $$2^{k+1} > (k+1)^2$$

  We know

  $$2^k 2 > 2k^2$$

  At this point if we can show that $2k^2 \geq (k+1)^2$ we are done, let's see if it's true

  $$k > 5 > 4$$
  $$(k-1)^2 > 9 > 2$$
  $$(k-1)^2 > 2$$
  $$k^2 - 2k + 1 > 2$$
  $$k^2 > 2k + 1$$
  $$2k^2 > (k+1)^2$$

  So it is true, therefore we can say

  $$2^{k+1} > (k+1)^2$$

  as required.

Thus by the principle of induction we have proven the original statement.   ■

Chapter 2

Lecture 2

2.1 Simple Induction Downfall

Observe if we are attempting to prove a statement, that requires us to know something more than just a property of the previous element we are proving over, for example a proof of prime factorization requires, us to know about all previous primes, this will become clear soon.

We will prove

$$\forall n \in \mathbb{N}, n \geq 2 \implies n \text{ has a prime factorization}$$

In our Induction Step we observe that we will have $k + 1 = a \cdot b$ where a, b are definelty not both $k + 1$, therefore , we will not be able to conclude anything about both of them, and we cannot proceed , therefore we need a stronger hypothesis.

Definition 2 (Complete Induction)
It is similar to Induction, with the following modifications

- *Base Case : show $P(b)$ holds*

- *Induction Step: let $k \in \mathbb{N}, k \geq b$ we assume the following our (Induction Hypothesis)*
$$P(b), P(b + 1), \ldots, P(k)$$

  Or equivalently, for $k \geq b$

$$\forall j \in \mathbb{N}, b \leq j \leq k, P(j)$$

We will prove the statement we tried earlier with simple induction.

Proof.
We define the following predicate

$$P(n) : \text{``} n \text{ has a prime factorization ''}, \text{ where } n \in$$

note, formally this means

$$n = \prod_{i=1}^{n} q_i$$

where $q_k \in \mathbb{N}$ and is prime .

- **Base Case:**
  We show that $P(2)$ holds, we know that 2 is a prime number , therefore it is itself a product of primes, as required.

- **Induction Step:**
  Let $k \in \mathbb{N}$ such that $k \geq 2$ and assume that $\forall j \in \mathbb{N}, 2 \leq j \leq k, P(j)$ holds, that is j has a prime factorization. We'll show that $P(k + 1)$ holds, so we must show that j has a prime factorization.

    - **Case 1**: j is prime, then we are done as it is already a product of primes.
    - **Case 2**: j is composite, that is there exists an $a, b \in \mathbb{N}$ such that , $j = ab$ also $a, b \neq 1 \wedge a, b \neq j$, we know that a and b cannot exceed j, or else $ab > j$ a contradiction same goes for b. Therefore $1 < a, b < j$ so by our Induction Hypothesis , they have a prime factorization. And thus we take the product of these two product of primes and j is then a product of primes.

Thus by the principle of complete induction we have proven the original statement.   ■

Note 2.1.1
observe in the above proof that an intricate part of the proof was to show that a, b where in fact in the correct range of the Induction Hypothesis, this is very important.

2.2   Common Problems in Complete Induction

We will prove
$$\forall n \in \mathbb{N}, n \geq 1, a_n = 2f_n - 1$$

Where

$$f_n = \begin{cases} 1, & \text{if } n = 1 \\ 1, & \text{if } n = 2 \\ \text{ otherwise }, f_{n-1} + f_{n-2} \end{cases}$$

$$a_n = \begin{cases} 1, & \text{if } n = 1 \\ 2, & \text{if } n = 2 \\ \text{otherwise } a_{n-1} + a_{n-2} + 1 \end{cases}$$

Proof.
We define the following predicate

$$P(n) : \text{"} a_n = 2f_n - 1 \text{"}, \text{ where } n \in \mathbb{N}$$

- **Base Case:**
  We show that $P(1)$ holds, we know

$$a_1 = 2f_1 - 1 \Leftrightarrow 1 = 2 - 1$$

  therefore $P(1)$ holds

  - Additional Base Case Required!
  - we show that $P(2)$ holds ,that is

$$1 = 2 - 1 \Leftrightarrow a_2 = 2f_2 - 1$$

- **Induction Step:**
  Let $k \in \mathbb{N}, k \geq \cancel{1}^{2}$ and assume that $\forall j \in \mathbb{N}, 1 \leq j \leq k, P(j)$ holds, that is

$$a_j = 2f_j - 1$$

  We'll show that $P(k+1)$ holds, so we must show that

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

  - **Case 1**: $k + 1 \geq 3$, if so we have

$$\begin{align} a_{k+1} &= a_k + a_{k-1} + 1 \qquad\qquad (\alpha) \\ &= 2f_k - 1 + (2f_{k-1} - 1) + 1 \\ &= 2f_k + 2f_{k-1} - 1 \\ &= 2(f_k + f_{k-1}) - 1 \\ &= 2f_{k+1} - 1 \end{align}$$

  - **Case 2**: $k + 1 \leq 2 \Leftrightarrow k = 1$

$$a_2 = 2f_2 - 1 \Leftrightarrow 1 = 1$$

We know

Thus by the principle of complete induction we have proven the original statement.   ∎

The above proof may have seemed, fine, though there is a problem. $k \geq 1$ so $k - 1 \geq 0$, though we we only have information about $P(j)$, for $j \in \{1, \ldots, k\}$. Therefore we necessarily require, $k - 1 \geq 1$ so that it is contained within the Induction Hypothesis bounds, that is true if and only if $k \geq 2$, so we add an additional Base Case to cover the gap we created.

2.2.1   Looking for Flaws in Strong Induction

When looking for flaws, whenever the Induction Hypothesis is used, you must verify that in fact is in the correct range. If we have a proof by induction and our Induction Hypothesis assumed over $0, \ldots k$ and in our algebra we have used the Induction Hypothesis on $k - 1$, then we know this will cause problems, so then we must say $k - 1 \geq 0 \Leftrightarrow k \geq 1$ and thus we must fill in the extra base case, usually if the statement is false, then this is what causes a contradiction.

2.2.2   Induction on Different Sets

- We can induct on the set of even natural numbers, say we prove $P(0)$, and also $P(k) \implies P(k + 2)$ then we get all even numbers.

- $P(0)$ and we show the following

$$P(k) \implies P(k+1) \qquad\qquad P(k) \implies P(k-1)$$

- Recall that there is no smallest rational number, and that the sum of two rational numbers is also a rational number, therefore there is no smallest increment that we can induct on, so I believe we cannot induct over $\mathbb{Q}$

Chapter 3

Preliminaries

3.1 Sets

- We now have the concept of the cardinality of a set being infinity that is for a set A we have, $|A| = \infty$

- ∞: for all integers k we have $k < \infty$

- Describing by listing all elements explicitly is called an <u>extensional</u> description, we can state the property that characterises it's elements, then we have an <u>internal</u> description (set-builder).

- A <u>proper</u> sub/super $A \subset B$ set means that every element of A is also an element of B moreover, there is at least one element of B that is not in A.

- If $A \cap B = \emptyset$, that is A and B have nothing in common, then we say they are <u>disjoint</u>.

- The difference of $A - B$ is the set of elements in A, that don't belong to B

- The intersection or union of an arbitary number, or infinite number of sets, is written as (I is a set of indicies)

$$\cup_{i \in I} A_i = \{x : \text{ for some } i \in I, x \in A_i\}$$
$$\cap_{i \in I} A_i = \{x : \text{ for each } i \in I, x \in A_i\}$$

- Partition: For a set A a partition of A is a set, that satisifies the following.

  - $\mathcal{X} \subseteq \mathcal{P}(A)$ such that $X \in \mathcal{X}, \mathcal{X} \neq \emptyset$
  - $X, Y \in \mathcal{X}$ such that $X \neq Y, X \cap Y = \emptyset$ and $\cup_{X \in \mathcal{X}} X = A$

3.1.1   Ordered Pairs

- Ordered pairs actually can be defined more primitively, we have (a, b) we can define it as the set $\big\{\{a\}, \{a, b\}\big\}$, the element that is of length 1, is viewed as the first element of the ordered set, the element of size two represents the ordered pair, one of which is the first, and the other is the second.

- For example if we have $(j, k) = (l, m)$, then $\big\{\{j\}, \{j, k\}\big\} = \big\{\{l\}, \{l, m\}\big\}$ therefore we must verify that they are subsets of eachother.