MAT236 - Intro to the Theory of Computation

Callum Cassidy-Nolan

September 17, 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

$$P(n) : \text{“}n \textit{ is an odd natural number}\text{”}, \textit{ where } n \in \mathbb{N}$$

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

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

■

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

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

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

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

- **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

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

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

  $$\begin{gathered} k > 5 > 4 \\ (k-1)^2 > 9 > 2 \\ (k-1)^2 > 2 \\ k^2 - 2k + 1 > 2 \\ k^2 > 2k + 1 \\ 2k^2 > (k+1)^2 \end{gathered}$$

  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

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

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

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

- **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 $k \in \mathbb{N}, k \geq 2$ 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

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

  - **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

Lecture 3

3.1 Induction on Word Problems

- Identify the statement we must prove, in the Aaron and Bianca problem our predicate was defined in english as so
  - $P(n)$: given the rules of the game & assuming the games starts with two pies, each with n matches. If Aaron goes first then Bianca has a winning strat.

  Note 3.1.1
  We require a variable that represents the size of the problem

- For the second quesiton we had a sum with variables n, m like

$$\sum_{i=0}^{n}(m)^i$$

  and that if we increase m in our induction step then it's quite hard to simply, and so we just induct on n and prove like

$$\forall n \in \mathbb{N}, m \geq 2 \implies \dots$$

Definition 3 (Well Ordering Principle)
Any subset A of $\mathbb{N}$ contradiction contains a minimum element that is for all $A \subseteq \mathbb{N}$ such that $A \neq \emptyset$ there exists an $a \in A$, such that $\forall b \in A, a \leq b$

Example 3.1.1
X : The set of odd natural numbers, $X \subseteq \mathbb{N}, X \neq \emptyset$ by the Well Ordering Principle , X has a minimum element namely 1.

Theorem 1 (Well Ordering Principle and Induction Equivalence)
The Well Ordering Principle, Principle of Mathematical Induction and Complete induction are equivalent.

$$PSI \Leftrightarrow WOP \Leftrightarrow PCI$$

that is if we have proof using simple induction, then we can also prove it with Well Ordering Principle or complete induction.

3.2 Well Ordering Principle Proof

we will prove

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

We define the predicate $P(n)$:

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

Proof.
For contradiction sake, we assume the negation of the statement we want to prove that is

$$\exists k \in \mathbb{N} \text{ such that } \neg P(k)$$

- Let S be a set of natural numbers j such that $j \in S$ if and only if $\neg P(j)$
  - if $j \in S \implies \neg P(j)$
  - if $j \notin S \implies P(j)$
- observe $k \in S$ therefore $S \neq \emptyset$ and by definition $S \subseteq \mathbb{N}$ therefore by the Well Ordering Principle there exists a minimum element of S Let a be said element.
- Claim: $a > 0 \Leftrightarrow a \geq 1$, observe

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

  so $P(0)$ holds, thus by definition $0 \notin S$
- since $S \subseteq \mathbb{N}$ & a is the minimum elements of S then $a > 0 \Leftrightarrow a \geq 1$ therefore

  $$a - 1 \geq 0 \text{ and } a - 1 \in \mathbb{N}$$

- Recall a is the minimum element of S therefore $a - 1 \in S$ so by the definition of S $P(a-1)$ holds that is

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

- But then $P(a)$ holds , but $a \in S$ so by definition $\neg P(n)$ holds, thus a contradiction so then our original statement is false and

  $$\forall n \in \mathbb{N}, P(n)$$

■

3.3 Well Ordering Principle Comments

- The base case is similar to shoiwng $a > 0$
- Induction Step is simliar to $P(a-1) \implies P(a)$ giving a contradiction.

Steps Involved

1. define predicate
2. Assume for contradiction $\neg\big(\forall n \in \mathbb{N}, P(n)\big)$
3. Define S such that $k \in S \Leftrightarrow \neg P(k)$ so
$$S = \big\{k \in \mathbb{N} : \neg P(k)\big\}$$
4. Show by assumption $S \neq \emptyset$
5. Use Well Ordering Principle to get smallest element of S
6. Reach contradiction using a and values less than a that hold so you can get $P(x) \implies P(a)$ which gives a contradiction.
7. Conclude the original assumption is false

Note 3.3.1
The last steps aren't always the same and require creativity

3.4 Harder Well Ordering Principle Proof

We will prove that every natural number has a prime factorization we define the predicate

$$P(n) : \text{“}n \text{ has a prime factorization ”, where } n \in \mathbb{N}$$

Proof.
assume for the sake of contradiction that there exists an $x \in \mathbb{N}, x \geq 2$ such that $\neg P(x)$

- Let S be the a subset of the natural numbers $j \geq 2$ such that $j \in S$ if and only if $\neg P(j)$
- Observe $S \neq \emptyset$ since $x \in S$, therefore by the Well Ordering Principle there exists a $c \in S$ such that c is the minimum element of S
- Observe that no prime could be in S as a prime number has a prime factorization, that is just itself. Therefore we know c is not prime, that is it is composite so there exists $a, b \in \mathbb{N}$ such that

  $$a \cdot b = c \text{ and } 1 < a, b < c$$

  since $a, b \leq c$ then $a, b \notin S$ thus $P(a) \wedge P(b)$ hold, so they have a prime factorization so

  $$a = p_1 p_2 \cdots p_{k-1} p_k \text{ and } b = r_1 r_2 \cdots r_{s-1} r_s$$

  and so

  $$c = p_1 p_2 \cdots p_{k-1} p_k \cdot r_1 r_2 \cdots r_{s-1} r_s$$

  So c can be written as a product of primes therefore $P(c)$ holds , but $c \in S$ so by definition $\neg P(c)$ thus a contradiction and so the original assumption is false, os

$$\forall n \in \mathbb{N}, n \geq 2 \implies P(n)$$

■

Note 3.4.1
Notice the last step is very simliar to induction, and the fact that $c \geq 2$ wouldn't help with the proof and we needed something stronger in order to prove the statement, note that coming up with this property of c that leads to a contradiction is hard and takes time.

Chapter 4

Preliminaries

4.1 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 extensional description, we can state the property that characterises it's elements, then we have an internal description (set-builder).
- A proper 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 disjoint.
- 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 $\cup_{X \in \mathcal{X}} X = A$

4.1.1 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.