6.1 Mathematical Induction

Notebook:	Discrete Mathematics [CM1020]		
Created:	2019-10-07 2:31 PM	**Updated:**	2019-12-02 1:40 PM
Author:	SUKHJIT MANN		

Cornell Notes	**Topic:** 6.1 Mathematical Induction	Course: BSc Computer Science Class: Discrete Mathematics-Lecture Date: December 02, 2019

Essential Question:

What are proofs & mathematical induction?

Questions/Cues:

- What is a proof?
- What is a direct proof?
- What is proof by contrapositive?
- What is proof by contradiction?
- What is Mathematical induction?
- What is the intuition behind induction?
- What is the structure of induction?
- What are the uses of induction?
- What is strong induction?
- What is strong induction sometimes otherwise known as?
- What is the well-ordering property?
- What the equivalence between mathematical induction, well-ordering property & strong induction?

Notes

Definition

- A **proof** is a valid argument that is used to prove the truth of a statement
- To **build** a **proof** we need to use all the **blocks** we have introduced previously:
  - Variables and predicates
  - Quantifiers
  - Laws of logic
  - Rules of inference

Terminology

We need to define some terms, even if choosing the appropriate term is intrinsically subjective:

- A **theorem** is a formal statement that can be shown to be true
- An **axiom** is a statement we assume to be true to serve as a premise for further arguments
- A **lemma** is a proven statement used as a step to a larger result rather than as a statement of interest by itself
- A **corollary** is a theorem that can be established by a short proof from a theorem.

Formalising a theorem

- Let's consider the statement **S**: "There exists a real number between any two not equal real numbers."
- **S** can be **formalised** as: $\forall x, y \in \mathbb{R}$ if $x < y$ then $\exists z \in \mathbb{R}$ where $x < z < y$
- **S** is a **theorem.**

Direct proof

- A **direct proof** is based on showing that a conditional statement: $p \rightarrow q$ is true
- We start by assuming that p is true and then use: **axioms, definitions** and **theorems,** together with **rules of inference,** to show that q must also be true.

Example

Let's give a proof of the theorem:

"There exists a real number between any two not equal real numbers."

Proof:

- Let x, y be arbitrary elements in $\mathbb{R}$
- Let's suppose $x < y$
- Let $z = (x + y)/2$
- $z \in \mathbb{R}$, satisfying $x < z < y$

∴ Therefore, using the universal generalisation rule, we can conclude that:
$\forall x, y \in \mathbb{R}$ if $x < y$ then $\exists z \in \mathbb{R}$ where $x < z < y$

Proof by contrapositive

- A **proof by contrapositive** is based on the fact that proving the conditional statement $p \rightarrow q$ is equivalent to proving its contrapositive: $\neg q \rightarrow \neg p$

- We start by assuming that $\neg q$ is true and then use: **axioms, definitions** and **theorems**, together with **rules of inference**, to show that $\neg p$ must also be true.

Example

Let's give a proof of the theorem:
"If n^2 is even then n is even."

Proof:

- **Direct** proof :
  - Let $n \in \mathbb{Z}$. If n^2 is even then $\exists k \in \mathbb{Z}$, $n^2 = 2k$
  - Then $\exists k \in \mathbb{Z}$, $n = \pm\sqrt{2k}$. From this equation it doesn't seem intuitive to prove that n is even.

- Proof by **contraposition:**
  - Let's suppose n is odd
  - Then $\exists k \in \mathbb{Z}$, $n = 2k+1$
  - Then $\exists k \in \mathbb{Z}$, $n^2 = (2k+1)^2 = 2(2k^2+2k)+1$
  - Then n^2 is also odd
  - We have succeeded in proving the contrapositive: if n is odd then n^2 is odd.

Proof by contradiction

- A **proof by contradiction** is based on assuming that the statement we want to prove is **false**, and then showing that this assumption leads to a **false** proposition

- We start by assuming that ¬p is true and then use: **axioms**, **definitions** and **theorems**, together with **rules of inference**, to show that ¬p is **false**. We can then conclude that it was wrong to assume that p is **false**, so it must be **true**.

Example

Let's give a direct proof of the theorem:
"There are infinitely many prime numbers."

Proof:

- Let's suppose there are only finitely many prime numbers
- Let's list them as $p_1, p_2, p_3, \ldots, p_n$ where $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ and so on
- Let's consider the number $c = p_1 p_2 p_3 \cdots p_n + 1$, the product of all the prime numbers, plus 1
- Then, as c is a natural number, it has at least one prime divisor.
- Then $\exists k \in \{1 \ldots n\}$, where p_k / c
- Then $\exists k \in \{1 \ldots n\}$, $\exists d \in \mathbb{N}$ where $dp_k = c = p_1 p_2 p_3 \cdots p_n + 1$
- Then $\exists k \in \{1 \ldots n\}$, $\exists d \in \mathbb{N}$ where $d = p_1 p_2 \cdots p_{k-1} p_{k+1} \cdots p_n + \frac{1}{p_k}$
- Then, $\frac{1}{p_k}$, in the expression above, is an integer, which is a contradiction.

Definition

- Mathematical induction can be used to assert that a propositional function P(n) is true for all positive integers n.

- **The rule of inference:**

$$\begin{array}{l} P(1) \text{ is true} \\ \forall k \ (P(k) \rightarrow P(k+1)) \\ \hline \therefore \forall n \ P(n) \end{array}$$

The intuition behind induction

- Let P(n) be the propositional function verifying:
  - P(1) is true
  - $\forall k \ (P(k) \rightarrow P(k+1))$
- **Intuitively:**
  - P is true for 1
  - Since P is true for 1, it's true for 2
  - Since P is true for 2, it's true for 3
  - And so on …
  - Since P is true for n-1, it's true for n …
- **In other words:**
  - The base case shows that the property initially holds true
  - The inductive step shows how each iteration influences the next one.

Structure of induction

In order to prove that a propositional function P(n) is true for all, we need to verify two steps:

1. **BASIS STEP**: where we show that P(1) is true
2. **INDUCTIVE STEP**: where we show that for $\forall k \in \mathbb{N}$:
   if P(k) is true, called **inductive hypothesis**,
   then P(k + 1) is true.

Some uses of induction

Mathematical induction can be used to prove P(n) is true for all integers greater than a particular integer, where P(n) is a propositional function. That might cover multiple cases such as:

- Proving formulas
- Proving inequalities
- Proving divisibility
- Proving properties of subsets and their cardinality.

Proving formulas

- Let's start by proving a simple formula formalised as the propositional function, P(n): $1+2+3+...+n = n(n+1)/2$

- In order to prove that a propositional function P(n) is true for all, we need to verify two steps :

1. **BASIS STEP**: where we show that P(1) is true

2. **INDUCTIVE STEP**: where we show that for $\forall k \in \mathbb{N}$:
   if P(k) is true, called **inductive hypothesis**,
   then P(k + 1) is true.

Example

1. **BASIS STEP**: The basis step, P(1) reduces to $1 = 1(1+1)/2$

2. **INDUCTIVE STEP**:
   - Let $\forall k \in \mathbb{N}$
   - If the inductive hypothesis P(k) is true:
     - we have $1+2+3+...+k = k(k+1)/2$
     - then, $1+2+3+...+k+(k+1)$
       $= k(k+1)/2+(k+1)$
       $= (k(k+1)+2(k+1))2$
       $= (k+1)\ ((k+1) + 1)\ /2$
     - which verifies, P(k+1).

Proving inequalities

- We may also use mathematical induction to prove an inequality that holds for all positive integers greater than a particular positive integer

- Let's consider proving the propositional function P(n): $3^n < n!$ if n is an integer greater than or equal to 7.

Example

1. **BASIS STEP**: The basis step, P(7) reduces to $3^7 < 7!$ because 2187 < 5040.

2. **INDUCTIVE STEP**:
   - Let $k \in \mathbb{N}$ and $k \geq 7$
   - If the inductive hypothesis P(k) is true:
     then, $3^{k+1} = 3 * 3^k <$ (k+1) *k! = (k+1)! which verifies P(k+1) is true.

Proving divisibility

- We may also use mathematical induction to prove a divisibility that holds for all positive integers greater than a particular positive integer.

- Let's consider proving the propositional function P(n): $\forall n \in \mathbb{N}$ 6^n**+4 is divisible by 4**

Example

1. **BASIS STEP**: The basis step, P(0) reduces to $6^0 + 4$ is divisible by 5, because $6^0 + 4 = 5$

2. **INDUCTIVE STEP**:
   - Let $k \in \mathbb{N}$
   - If the inductive hypothesis P(k) is true:
     - then, $6^k + 4 = 5$p, where $p \in \mathbb{N}$
     - then, $6^{k+1} + 4 = 6 * (5p - 4)$+4
       $= 30p - 20$
       $= 5(6p - 4)$ which is divisible by 5 and verifies P(k+1) is true.

Incorrect Induction

Let's consider the statement of the following incorrect induction: P(n): $\forall n \in \mathbb{N} \sum_{i=0}^{n-1} 2^i = 2^n$

Proof:

- Let k ∈ ℕ. Let's suppose the inductive hypothesis P(k) is true, which means : $\sum_{i=0}^{k-1} 2^i = 2^k$
- Now let's examine P(k+1)
- $\sum_{i=0}^{k} 2^i = \sum_{i=0}^{k-1} 2^i + 2^k = 2^k + 2^k = 2^{k+1}$
- This means that P(k+1) is also true and verifies the induction step.

Incorrect induction

- Even though we have been able to prove the induction step, let's prove that the statement: $\forall n \in \mathbb{N}$ $\sum_{i=0}^{n-1} 2^i = 2^n$ is FALSE
  - For example $2^0 + 2^1 = 3$ which is different from 2^2
- Our reasoning seemed correct because we haven't verified the base case and have made **false assumptions**
- In other words, and as we saw in propositional logic, false assumptions imply false conclusions
- To avoid this situation we need to make sure both the **base case** and the **inductive step** are verified.

Strong induction

- Sometimes, it is easier to prove statements using a different form of mathematical induction, called strong induction
- Strong induction can be formalised using the following **rule of inference**:

$$\frac{\begin{array}{l} P(1) \text{ is true} \\ \forall k \in \mathbb{N} \quad P(1), P(2) \ldots P(k) \rightarrow P(k+1) \end{array}}{\therefore \forall n \in \mathbb{N}, P(n)}$$

- Strong induction is sometimes called the second principle of mathematical induction or complete induction

Example

Let's start by proving a simple statement, expressed as the propositional function, P(n): $\forall n \in \mathbb{N}$ and $n \geq 2$, n is divisible by a prime number.

- To prove it, we need to verify two steps:

1. **BASIS STEP**: The basis step, P(2) reduces to 2, which is divisible by a prime number because 2 is a prime number and divides itself.

2. **INDUCTIVE STEP**:
   - Let $k \in \mathbb{N}$, greater than 2.
   - If the inductive hypothesis is P(k) is true:
     - let's also assume P(2) ... P(k+1) is true. Then, $\forall m \in \mathbb{N}$ and $2 \leq m \leq k+1$: $\exists p$ is a prime number dividing m
     - We have two cases:
       - k+2 is a prime number, in which case it is trivially divisible by itself
       - k+2 is not a prime number, in which case $\exists m$ dividing $k + 2$
       - *as* $2 \leq m \leq k+1$, $\exists p$ is a prime number dividing m. p also divides k+2
       - Which verifies P(k+2) is true and proves the strong induction.

Well-ordering property

The well-ordering property is an axiom about $\mathbb{N}$ that we assume to be true. The axioms about $\mathbb{N}$ are the following:

1. The number 1 is a positive integer
2. If $n \in \mathbb{N}$, then $n + 1$, the successor of n, is also a positive integer
3. Every positive integer other than 1 is the successor of a positive integer
4. The well-ordering property: every nonempty subset of the set of positive integers has at least one element.

The well-ordering property can be used as a tool in building proofs.

Example

Let's reconsider the earlier statement P(n): $\forall n \in \mathbb{N}$ and $n \geq 2$, n is divisible by a prime number.

- **Proof:**
  - Let S be the set of positive integers greater than 1 with **no prime divisor**
  - Suppose S is nonempty. Let n be its smallest element
  - n cannot be prime, since n divides itself and if **n** were prime, it would be its own prime divisor
  - So n is composite: it must have a divisor d with $1<d<n$. Then, d must have a prime divisor (by the minimality of n), let's call it p
  - Then p/d and d/n, so p/n, which is a contradiction
  - Therefore S is empty, which verifies P(n).

Equivalence of the three concepts

We can prove the following statements:
- mathematical induction → the well-ordering property
- the well-ordering property → strong induction
- strong induction → mathematical induction.

- That is, the principles of mathematical induction, strong induction and well-ordering are all equivalent

- In other words, the validity of each of these three proof techniques implies the validity of the other two techniques.

Summary

In this week, we learned what a proof is, the different types of proofs & what mathematical induction is. Also we looked a different form of induction called strong induction, the structure of induction, the well-ordering property & the equivalence of mathematical induction, the well-ordering property & strong induction.