MODULE 3: DEFINITIONS, THEOREM AND PROOFS
WEEK 3

Learning Outcomes:

After completing this course you are expected to demonstrate the following:

1. Discuss the three entities of mathematical subject and its use in automata theory.

A. Engage

Trivia

Theorems and proofs are the heart and soul of mathematical and definitions are its spirit. These three entities are central to every mathematical subject, including ours.

B. Explore

Video Title: **Mathematical Video**
YouTube Link: **https://www.youtube.com/watch?v=S0DSM-EkQE8**
Module Video Title: **Week 3 - Mathematical Video**

C. Explain

Definitions describe the objects and notation that we use. A definition may be simple, as in the definition of set given earlier in the module 2, or complex as in the definition of security in a cryptographic system. Precision is essential to any mathematical definition. When defining some object, we must make clear what constitutes that object and what does not.

A **proof** is a convincing logical argument that a statement is true. In mathematical an argument must be airtight that is, convincing in an absolute sense. In everyday life or in the law, the standard of proof is lower.

A **theorem** is a mathematical statement proved true. Generally, we reserve the use of the word for statements of special interest. Occasionally we prove statements that are interesting only because they assist in the proof if another, more significant statements.

D. Elaborate

Four Fundamental Proof Techniques:

1. Direct Proof (Proof by Construction)

In a constructive proof one attempts to demonstrate P ⇒ Q directly. This is the simplest and easiest method of proof available to us. There are only two steps to a direct proof (the second step is, of course, the tricky part):

- Assume that P is true.
- Use P to show that Q must be true.

Theorem 1. If a and b are consecutive integers, then the sum a + b is odd.

Proof. Assume that a and b are consecutive integers. Because a and b are consecutive, we know that b = a + 1. Thus, the sum a + b may be re-written as 2a + 1. Thus, there exists a number k such that a + b = 2k + 1 so the sum a + b is odd.

2. Proof by Contradiction

The proof by contradiction is grounded in the fact that any proposition must be either true or false, but not both true and false at the same time. We arrive at a contradiction when we are able to demonstrate that a statement is both simultaneously true and false, showing that our assumptions are inconsistent. We can use this to demonstrate P ⇒ Q by assuming both P and ¬Q are simultaneously true and deriving a contradiction. When we derive this contradiction, it means that one of our assumptions was untenable. Presumably we have either assumed or already proved P to be true so that finding a contradiction implies that ¬Q must be false.

The method of proof by contradiction.

- Assume that P is true.
- Assume that ¬Q is true. 3. Use P and ¬Q to demonstrate a contradiction.

Theorem 2. If a and b are consecutive integers, then the sum a + b is odd.

Proof. Assume that a and b are consecutive integers. Assume also that the sum a + b is not odd. Because the sum a + b is not odd, there exists no number k such that a + b = 2k + 1. However, the integers a and b are consecutive, so we may write the sum a + b as 2a + 1. Thus, we have derived that a + b 6= 2k + 1 for any integer k and also that a + b = 2a + 1. This is a contradiction. If we hold that a and b are consecutive then we know that the sum a + b must be odd.

3. Proof by Induction

Proof by induction is a very powerful method in which we use recursion to demonstrate an infinite number of facts in a finite amount of space. The most basic form of mathematical induction is where we first create a propositional form whose truth is determined by an integer function. If we are able to show that the propositional form is true for some integer value then we may argue from that basis that the propositional form must be true for all integers.

1. Show that a propositional form P(x) is true for some basis case.
2. Assume that P(n) is true for some n, and show that this implies that P(n + 1) is true.
3. Then, by the principle of induction, the propositional form P(x) is true for all n greater or equal to the basis case.

Theorem 3. If a and b are consecutive integers, then the sum a + b is odd.

Proof. Define the propositional form F(x) to be true when the sum of x and its successor is odd. (Step 1) Consider the proposition F(1). The sum 1 + 2 = 3 is odd because we can

demonstrate there exists an integer k such that 2k + 1 = 3. Namely, 2(1) + 1 = 3. Thus, F(x) is true when x = 1. 2 (Step 2) Assume that F(x) is true for some x. Thus, for some x we have that x + (x + 1) is odd. We add one to both x and x + 1 which gives the sum (x+1)+(x+2). We claim two things: first, the sum (x+1)+(x+2) = F(x+1). Second, we claim that adding two to any integer does not change that integer's evenness or oddness. With these two observations we claim that F(x) is odd implies F(x + 1) is odd. (Step 3) By the principle of mathematical induction we thus claim that F(x) is odd for all integers x. Thus, the sum of any two consecutive numbers is odd.

4. Proof by Contrapositive

Proof by contraposition is a method of proof which is not a method all its own per se. From first-order logic we know that the implication P ⇒ Q is equivalent to ¬Q ⇒ ¬P. The second proposition is called the contrapositive of the first proposition. By saying that the two propositions are equivalent we mean that if one can prove P ⇒ Q then they have also proved ¬Q ⇒ ¬P, and vice versa.

Proof by contraposition can be an effective approach when a traditional direct proof is tricky, or it can be a different way to think about the substance of a problem.

Theorem 4. If the sum a + b is not odd, then a and b are not consecutive integers. It is important to be extremely pedantic when interpreting a contraposition. It would be tempting to claim that the above theorem claims that the sum of two numbers is odd only when those two numbers are consecutive. However, this is nonsense.

Proof. Assume that the sum of the integers a and b is not odd. Then, there exists no integer k such that a + b = 2k + 1. Thus, a + b 6= k + (k + 1) for all integers k. Because k + 1 is the successor of k, this implies that a and b cannot be consecutive integers.

Examples:

1. Direct Proof

There are two steps to directly proving P ⇒ Q:

1. Assume P is true.
2. Demonstrate that Q must follow from P.

Definition 4. Let MAX(a, b) be a function which returns whichever of a or b is greater.

Definition 5. Let ABS(a) be defined to be such that if a is positive then ABS(a) = a, and if a is negative then ABS(a) = −a.

The following proofs demonstrate that sometimes it's easiest to break a proposition into separate cases and prove each case separately.

Theorem 5. Let a, b , c, d be integers. If a > c and b > c, then MAX(a, b) − c is always positive.

Proof. Assume that a > c and b > c. We know that a > c and b > c, but we cannot say for certain if a > b or b > a. Therefore we proceed by cases.

1. Case 1: Assume that a > b. Because a > b we know that MAX(a, b) = a. We may thus claim that MAX(a, b) − c = a − c. By assumption we know that a > c so the difference a − c must be positive.

2. Case 2: Assume that b > a. Because b > a we know that MAX(a, b) = b. We may thus claim that MAX(a, b) − c = b − c. By assumption we know that b > c so the difference b − c must be positive. Thus, in all possible cases MAX(a, b) − c is positive.

Theorem 6. If a and b are integers, then ABS(a)ABS(b) = ABS(ab).
Proof. Assume that a and b are integers. We proceed by cases:

1. Case 1: Suppose a is negative and b is positive. By definition ABS(a) = −a and ABS(b) = b. Thus, ABS(a)ABS(b) = −ab. Likewise, the product ab is negative so ABS(ab) = −ab. Thus, ABS(a)ABS(b) = ABS(ab).

2. Case 2: Suppose that a is positive and b is negative. By definition ABS(a) = a and ABS(b) = −b. Thus, ABS(a)ABS(b) = a(−b) = −ab. Likewise, the product ab is negative so ABS(ab) = −ab. Thus, ABS(a)ABS(b) = ABS(ab).

3. Case 3: Suppose that both a and b are positive. By definition ABS(a) = a and ABS(b) = b. Thus, ABS(a)ABS(b) = ab. Likewise, the product ab is positive so ABS(ab) = ab. Thus, ABS(a)ABS(b) = ABS(ab).

4. Case 4: Suppose that both a and b are negative. By definition ABS(a) = −a and ABS(b) = −b. Thus, ABS(a)ABS(b) = (−a)(−b) = ab. Likewise, the product ab is then positive so ABS(ab) = ab. Thus, ABS(a)ABS(b) = ABS(ab). Therefore, in every possible case we have that ABS(a)ABS(b) = ABS(ab).

2. Proof by Contradiction

Steps to proving a theorem by contradiction:

1. Assume P is true.
2. Assume ¬Q is true.
3. Demonstrate a contradiction.

The statement of the following proof is different from those we have seen so far in that there is no explicitly stated starting assumption. In these cases, we are free to assume we have at our disposal the general machinery of the subject which we are studying. In this case, we implicitly assume all of number and set theory to tackle the problem.

Theorem 7. Prove that there are an infinite number of primes.
Proof. Assume, by way of contradiction, that there are a finite number of primes p1, p2, p3...pn. Let k be the product of all these primes plus one: k = p1p2p3...pn + 1. The integer k is clearly

greater than one and because k is an integer, there must exist some prime number P which divides it. However, P cannot be any one of p1, p2, p3...pn because if it were then P could divide the difference k − p1p2p3...pn and k − p1p2p3...pn = 1. P cannot divide one and also be prime (which is by definition greater than one). This is a contradiction. Therefore, our assumption is false so there must be an infinite number of primes.

3. Proof by Mathematical Induction

To demonstrate P ⇒ Q by induction we require that the truth of P and Q be expressed as a function of some ordered set S.

1. (Basis) Show that P ⇒ Q is valid for a specific element k in S.
2. (Inductive Hypothesis) Assume that P ⇒ Q for some element n in S.
3. Demonstrate that P ⇒ Q for the element n + 1 in S.
4. Conclude that P ⇒ Q for all elements greater than or equal to k in S.

Theorem 8. Show that the summation formula

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

is valid for all integers n.

Proof. (*Basis case*) We demonstrate that the formula is valid for n = 1. By substituting one for n the formula gives us 1 = 1(2) 2 , which is true.

(*Inductive Hypothesis*) Suppose that the formula is valid for some integer n. To demonstrate that the formula is valid for n + 1 we must use the inductive hypothesis to show that the formula still holds.

By assumption the formula is valid for n. Using basic algebra, we add n + 1 to both sides of the equation to demonstrate that the formula is still valid for n + 1. We begin with the left-hand side:

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

We now demonstrate adding n + 1 to the right hand side. We perform fraction addition and factor out an(n + 1).

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

Combining the right-hand sides of equations two and three yields:

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

Which is exactly what we require. Thus, if the formula is valid for n then the formula must be valid for n + 1 as we have shown above.

Thus, by mathematical induction over the integers, the summation formula is valid for all integers greater than or equal to one.

4. Proof by Contrapositive

Recall that first-order logic shows that the statement P ⇒ Q is equivalent to ¬Q ⇒ ¬P.

1. Assume ¬Q is true.
2. Show that ¬P must be true.
3. Observe that P ⇒ Q by contraposition.

Logically, a direct proof, a proof by contradiction, and a proof by contrapositive are all equivalent. It is also true that if in general you can find a proof by contradiction then you can also find a proof by contrapositive. After you have proved a proposition by contradiction you might surprise yourself by converting the contradiction proof to a contrapositive proof. The reason is that in both cases we assume that ¬Q is true and argue from that point. In fact, oftentimes a proof by contradiction assumes ¬Q and argues towards ¬P!

Theorem 9. If x 2 is odd then x must be odd.

The above proof is certainly doable both by a direct proof or by a contradiction. However, a direct proof requires a cumbersome proof by cases approach and a contradiction is essentially arguing towards a proof by contrapositive. Remember to always state the contrapositive so your reader knows what you're arguing towards. Here I have taken a (justified) liberty with stating the contrapositive. Normally we would have to first prove that a" not odd" number must be even, but here I just claim this fact without proof.

Theorem 10. If x is even then x 2 is even.

Proof. We assume that x is even. By definition, there exists an integer k such that x = 2k. To derive the desired result, we square both sides which yields x 2 = 4k 2 = 2(2k 2). Thus, x 2 is even. Therefore, by proof of the contrapositive, if x 2 is odd then x must be odd

5. Evaluate

ASSESSMENT:
Instructions: You may write your answer on the Activity Sheet (ACTS) provided in this module.

CONTENT FOR ASSESSMENT:
Activity Number 2: (20-points)

1. If C is a set with elements, how many elements are in the power set of C?
2. Explain the condition that satifies the proof by mathematical induction.

References

1. *Basic Proof Techniques by David Ferry , September 13, 2010*
2. *Introduction to theTheory of Computation, 2nd edition*

Facilitated By:		
Name	:	
MS Teams Account (email)	:	
Smart Phone Number	:	