4. Methods of Proof

Aaron Tan

4.1 Direct Proof and Counterexample

- Definitions: even and odd numbers; prime and composite.
- Proving existential statements by constructive proof.
- Disproving universal statements by counterexample.
- Proving universal statements by exhaustion.
- Proving universal statements by generalizing from the generic particular.

4.2 Proofs on Rational Numbers

- Every integer is a rational number.
- Sum of any two rational numbers is rational.

4.3 Proofs on Divisibility

- Positive divisor of a positive integer; divisors of 1; transitivity of divisibility.

4.4 Indirect Proof

- Proof by contradiction; proof by contraposition.

Reference: Epp's Chapter 4 Elementary Number Theory and Methods of Proof

4.1 Definitions

4.1.1. Definitions

Assumptions

- In this text we assume a familiarity with the laws of basic algebra, which are listed in Appendix A.
- We also use the three properties of equality: For all objects A, B, and C, (1) $A = A$, (2) if $A = B$ then $B = A$, and (3) if $A = B$ and $B = C$, then $A = C$.
- In addition, we assume that there is no integer between 0 and 1 and that the set of all integers is closed under addition, subtraction, and multiplication. This means that sums, differences, and products of integers are integers.
- Of course, most quotients of integers are not integers. For example, $3 \div 2$, which equals $3/2$, is not an integer, and $3 \div 0$ is not even a number.

Appendix A has been uploaded onto “LumiNUS > Files > Lecture slides and notes” and the CS1231S website.

Recall from Lecture #2:

Definitions: Even and Odd Integers

An integer n is even if, and only if, n equals twice some integer.

An integer n is odd if, and only if, n equals twice some integer plus 1.

Symbolically, if n is an integer, then

$$n \text{ is even} \iff \exists k \in \mathbb{Z} \text{ such that } n = 2k.$$

$$n \text{ is odd} \iff \exists k \in \mathbb{Z} \text{ such that } n = 2k + 1.$$

Definitions: Prime and Composite

An integer n is prime iff $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n.

An integer n is composite iff $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

In symbols:

n is prime: $\forall r, s \in \mathbb{Z}^+,$

$$\big(n = rs \rightarrow (r = 1 \wedge s = n) \vee (r = n \wedge s = 1)\big).$$

n is composite: $\exists r, s \in \mathbb{Z}^+ \big(n = rs \wedge (1 < r < n) \wedge (1 < s < n)\big).$

CS1231S Midterm Test (AY2019/20 Sem1)

Given the following predicate:

$$P(x) = (x \neq 1) \wedge \forall y, z\,\big(x = yz \rightarrow ((y = x) \vee (y = 1))\big)$$

and that the domain of x, y and z is $\mathbb{Z}^+$, what is $P(x)$?

A. $P(x)$ is true iff x is a prime number.

B. $P(x)$ is true iff x is a number other than 1.

C. $P(x)$ is always true irrespective of the value of x.

D. $P(x)$ is true if x has exactly two factors other than 1 and x.

E. None of the above.

4.1.2. Proving Existential Statements by Constructive Proof

An existential statement:

$$\exists x \in D\ Q(x)$$

is true iff $Q(x)$ is true for at least one x in D.

To prove such statement, we may use constructive proofs of existence:

- Find an x in D that makes $Q(x)$ true; or
- Give a set of directions for finding such an x.

Example #1

a. Prove that there exists an even integer n that can be written in two ways as a sum of two prime numbers.

b. Suppose r and s are integers. Prove that there is an integer k such that $22r + 18s = 2k$.

a. Let $n = 10$. Then 10 = 5 + 5 = 3 + 7, where 3, 5 and 7 are all prime numbers.

Note that the question does <u>not</u> say that the two prime numbers must be distinct.

b. Let $k = 11r + 9s$. Then k is an integer because it is a sum of products of integers (by closure property); and $2k = 2(11r + 9s) = 22r + 18s$ (by distributive law).

4.1.3. Disproving Universal Statements by Counterexample

Given a universal (conditional) statement:

$$\forall x \in D \left(P(x) \rightarrow Q(x)\right).$$

Showing this statement is false is equivalent to showing that its negation is true.

The negation of the above statement is an existential statement:

$$\exists x \in D \left(P(x) \wedge \sim Q(x)\right).$$

To prove that an existential statement is true, we use an example (constructive proof), which is called the counterexample for the original universal conditional statement.

Disproof by Counterexample

To disprove a statement of the form

$$\forall x \in D\ \big(P(x) \rightarrow Q(x)\big),$$

find a value of x in D for which the hypothesis $P(x)$ is true but the conclusion $Q(x)$ is false.

Such an x is called a counterexample.

Example #2: Disprove the following statement

$$\forall a, b \in \mathbb{R}, \text{ if } a^2 = b^2 \text{ then } a = b.$$

Counterexample: Let $a = 1$ and $b = -1$. Then $a^2 = 1^2 = 1$ and $b^2 = (-1)^2 = 1$ and so $a^2 = b^2$. But $a \neq b$.

4.1.4. Proving Universal Statements by Exhaustion

Given a universal conditional statement:

$$\forall x \in D\ \big(P(x) \to Q(x)\big).$$

When D is finite or when only a finite number of elements satisfy $P(x)$, we may prove the statement by the method of exhaustion.

Example #3: Prove the following statement

$\forall n \in \mathbb{Z}$, if n is even and $4 \leq n \leq 26$, then n can be written as a sum of two primes.

Proof (by method of exhaustion):

- 4 = 2 + 2
- 6 = 3 + 3
- 8 = 3 + 5
- 10 = 5 + 5
- 12 = 5 + 7
- 14 = 11 + 3
- 16 = 5 + 11
- 18 = 7 + 11
- 20 = 7 + 13
- 22 = 5 + 17
- 24 = 5 + 19
- 26 = 7 + 19

4.1.5. Proving Universal Statements by Generalizing from the Generic Particular

The most powerful technique for proving a universal statement s one that works regardless of the size of the domain (possibly infinite) over which the statement is quantified.

Generalizing from the Generic Particular

To show that every element of a set satisfies a certain property, suppose x is a *particular* but *arbitrarily chosen* element of the set, and show that x satisfies the property.

Example #4: Prove that the sum of any two even integers is even.

Proof:

1. Let m and n be two particular but arbitrarily chosen even integers.

   1.1 Then $m = 2r$ and $n = 2s$ for some integers r and s (by the definition of even number)

   1.2 $m + n = 2r + 2s = 2(r + s)$ (by basic algebra)

   1.3 $2(r + s)$ is an integer (by closure of integers under $+$ and $\times$) and an even number (by the definition of even number)

   1.4 Hence $m + n$ is an even number.

2. Therefore the sum of any two even integers is even.

4.2 Proofs on Rational Numbers

4.2.1. Definition

In this section, we will apply proof techniques we have learned on rational numbers.

Definition: Rational Numbers

A real number r is rational if, and only if, it can be expressed as a quotient of two integers with a nonzero denominator.

A real number that is not rational is irrational.

$$r \text{ is rational } \iff \exists \text{ integers } a \text{ and } b \text{ such that } r = \frac{a}{b} \text{ and } b \neq 0.$$

4.2.2. Every Integer is a Rational Number

Theorem 4.2.1 (5^{th}: 4.3.1)

Every integer is a rational number.

Proof:

1. Let a be a particular but arbitrarily chosen integer.
   - 1.1 Then $a = \frac{a}{1}$ which is in the form $\frac{a}{b}$ where a and $b(= 1)$ are integers.
   - 1.2 Hence a is a rational number.
2. Therefore every integer is a rational number.

4.2.3. The Sum of Any Two Rational Numbers is Rational

Theorem 4.2.2 (5th: 4.3.2)

The sum of any two rational numbers is rational.

Proof:

1. Let r and s be two particular but arbitrarily chosen rational numbers.
   1.1 Then $r = \frac{a}{b}$ and $s = \frac{c}{d}$ for some integers a, b, c, d with $b \neq 0$ and $d \neq 0$ (by the definition of rational number).
   1.2 Then $r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ (by basic algebra).
   1.3 Since $ad + bc$ and bd are integers (by closure of integers under $+$ and $\times$) and $bd \neq 0$, so $r + s$ is rational.
2. Therefore the sum of any two rational numbers is rational.

Recall from Lecture #2:

Corollary

A result that is a simple deduction from a theorem.

Example:

- (Chapter 4)
  Theorem 4.2.2 (5th: 4.3.2) The sum of any two rational numbers is rational
  Corollary 4.2.3 (5th: 4.3.3) The double of a rational number is rational.

Theorem 4.2.2 (5th: 4.3.2)

The sum of any two rational numbers is rational.

Corollary 4.2.3 (5th: 4.2.3)

The double of a rational number is rational.

4.3 Proofs on Divisibility

4.3.1. Definition

Recall from Lecture #2:

Definition: Divisibility

If n and d are integers, then

n is divisible by d iff n equals d times some integer.

We use the notation $d \mid n$ to mean "d divides n". Symbolically, if $n, d \in \mathbb{Z}$:

$$d \mid n \Leftrightarrow \exists k \in \mathbb{Z} \text{ such that } n = dk.$$

4.3.2. Theorems

Theorem 4.3.1 (5th: 4.4.1) A Positive Divisor of a Positive Integer

For all positive integers a and b, if $a \mid b$, then $a \leq b$.

Proof (direct proof):

1. Let a and b be two positive integers and $a \mid b$.
   - 1.1 Then there exists an integer k such that $b = ak$ (by the definition of divisibility).
   - 1.2 Since both a and b are positive integers, k is positive, i.e. $k \geq 1$.
   - 1.3 Therefore $a \leq ak = b$.
2. Therefore for all positive integers a and b, if $a \mid b$, then $a \leq b$.

Theorem 4.3.2 (5th: 4.4.2) Divisors of 1

The only divisors of 1 are 1 and -1.

Proof (by division into cases):

1. Suppose m is any integer that divides 1.
   - 1.1 Then there exists an integer k such that $1 = mk$ (by the definition of divisibility).
   - 1.2 Since mk is positive, either both m and k are positive, or both negative.
   - 1.3 Case 1: Both m and k are positive.
     - 1.3.1 Since $m \mid 1$, $m \leq 1$ (by Theorem 4.3.1).
     - 1.3.2 Then $m = 1$.
   - 1.4 Case 2: Both m and k are negative.
     - 1.4.1 Then $-m$ is a positive integer divisor of 1, i.e. $-m|1$.
     - 1.4.2 By the same reasoning in 1.3.1 and 1.3.2, $-m = 1$, or $m = -1$.
2. Therefore the only divisors of 1 are 1 and -1.

Theorem 4.3.3 (5th: 4.4.3) Transitivity of Divisibility

For all integers a, b and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof:

1. Suppose a, b, c are integers s.t. $a \mid b$ and $b \mid c$.
   - 1.1 Then $b = ar$ and $c = bs$ for some integers r and s. (by the definition of divisibility)
   - 1.2 Then $c = bs = (ar)s$ (by substitution) $= a(rs)$ (by associativity)
   - 1.3 Let $k = rs$, then k is an integer (by closure property) and $c = ak$.
2. Therefore $a \mid c$.

4.4 Indirect Proof

4.4.1. Indirect Proof: Proof by Contradiction

Sometimes when a direct proof is hard to derive, we can try indirect proof.

Example: Theorem 4.7.1 (5^{th}: 4.8.1) $\sqrt{2}$ is irrational.

Proof by Contradiction

1. Suppose the statement to be proved, S, is false. That is, the negation of the statement, $\sim S$, is true.
2. Show that this supposition leads logically to a contradiction.
3. Conclude that the statement S is true.

Indirect Proof: Proof by Contradiction

Theorem 4.6.1 (5th: 4.7.1)

There is no greatest integer.

Proof (by contradiction):

1. Suppose not, i.e. there is a greatest integer.
   - 1.1 Let call this greatest integer g, and $g \geq n$ for all integers n.
   - 1.2 Let $G = g + 1$.
   - 1.3 Now, G is an integer (closure of integers under $+$) and $G > g$.
   - 1.4 Hence, g is not the greatest integer → contradicting 1.1.
2. Hence, the supposition that there is a greatest integer is false.
3. Therefore, there is no greatest integer.

4.4.2. Indirect Proof: Proof by Contraposition

Recall: Contrapositive of $p \to q$ is $\sim q \to \sim p$.

Proof by Contraposition

1. Statement to be proved: $\forall x \in D\ \big(P(x) \to Q(x)\big)$.
2. Rewrite the statement into its contrapositive form:

   $\forall x \in D\ \big(\sim Q(x) \to \sim P(x)\big)$.
3. Prove the contrapositive statement by a direct proof.

   3.1 Suppose x is an (particular but arbitrarily chosen) element of D s.t. $Q(x)$ is false.

   3.2 Show that $P(x)$ is false.
4. Therefore, the original statement $\forall x \in D\ \big(P(x) \to Q(x)\big)$ is true.

Recall that in Lecture 1, we use the following proposition to prove that $\sqrt{2}$ is irrational.

Proposition 4.6.4 (5th: 4.7.4)

For all integers n, if n^2 is even than n is even.

We shall now prove this proposition.

Proposition 4.6.4 (5th: 4.7.4)

For all integers n, if n^2 is even then n is even.

Proof (by contraposition):

1. Contrapositive statement:

   For all integers n, if n is odd then n^2 is odd.

2. Let n be an arbitrarily chosen odd number.

   2.1 Then $n = 2k + 1$ for some integer k (by definition of odd number).

   2.2 Then $n^2 = (2k + 1)(2k + 1) = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

   2.3 Let $m = 2k^2 + 2k$. Now, m is an integer (by closure property) and $n^2 = 2m + 1$.

   2.4 So n^2 is odd.

3. Therefore, for all integers n, if n^2 is even then n is even.

END OF FILE