MATH1061 Course Notes

Paddy Maher

August 24, 2021

1 Logic

1.1 Logical Connectives

1.1.1 Basic logical connectives

For a given logical statement come logical connectives. Basic logical connectives include:

- **not** $= \sim$
- **and** $= \wedge$
- **or** $= \vee$
- **exclusive or** $= \oplus$

1.1.2 Logical Equivalence

Given two statement forms, you can show that they are logically equivalent by using a truth table or by using the laws of logical equivalence.
The logical equivalence between two statements is demonstrated by the symbol $\equiv$

[insert truth table]

1.1.3 Conditional logical connectives

Logical connectives and equivalences, for given truth statements 'p' and 'q'

- **if .. then** $= \rightarrow$
- **if and only if** $= \leftrightarrow$
- $p \rightarrow q \equiv \sim p \vee q \equiv \sim q \rightarrow \sim p$

1.1.4 Order of Operations

1. $\sim$
2. $\wedge$ and $\vee$, use parentheses to specify. If no parentheses given, work from left to right.
3. $\rightarrow$ and $\leftrightarrow$, use parentheses to specify. If no parentheses given, work from left to right.

1.2 Necessary and sufficient conditions

For given truth statements 'p' and 'q':

- p is a necessary condition for q means "if $\sim p$ then $\sim q$" or equivalently "if q then p" or "q only if p".
- p is a sufficient condition for q means "if p then q" or equivalently "q if p"

1.3 Definitions

1.3.1 Tautology and contradictions

- A tautology is a statement form which always takes truth values "**true**" for all possible truth values of its variables.
- A contradiction is a statement form which always takes truth values "**false**" for all possible truth values of its variables.

1.3.2 Contrapositive

For given truth statements 'p' and 'q'
The contrapositive of $p \to q$ is $\sim q \to \sim p$

- These are logically equivalent:
  $p \to q \equiv \sim q \to \sim p$

1.3.3 Biconditional

For given truth statements 'p' and 'q'
The biconditional of p and q, denoted $p \leftrightarrow q$, is defined by the following truth table:

[insert truth table]

1.4 Arguments

1.4.1 Premises

Given a collection of statements '$p_1, p_2, ..., p_n$' (called **premises**) and another statement 'q' (called the conclusion), an '*argument*' is the assertion that the conjunction of the premisees implies the conclusion.

$$p_1$$
$$p_2$$
$$...$$
$$p_n$$
$$\therefore q$$

1.4.2 Arguments; validity and invalidity

Definition; valid argument An argument is **valid** if whenever all of the premises are true, the conclusion is also true.

Thus, an argument is valid if $(p_1 \wedge p_2 \wedge ... \wedge p_n \to q)$ is a tautology.

Definition; invalid argument An argument is **invalid** if it is possible to have a situation in which all of the premises are true but the conclusion is false.

We can check whether an argument is valid or invalid using a truth table.

1.4.3 Rules of Inference

Modus Ponens

$$p \to q$$
$$p$$
$$\therefore q$$

Modus Tollens

$$p \to q$$
$$\sim q$$
$$\therefore \sim p$$

Generalisation

$$p$$
$$\therefore p \vee q$$

$$q$$
$$\therefore p \vee q$$

Specialisation

$$p \wedge q$$
$$\therefore p$$

$$p \wedge q$$
$$\therefore q$$

Conjunction

$$p$$
$$q$$
$$\therefore p \wedge q$$

Elimination

$$p \vee q$$
$$\sim q$$
$$\therefore p$$

$$p \vee q$$
$$\sim p$$
$$\therefore q$$

Transitivity

$$p \to q$$
$$q \to r$$
$$\therefore p \to r$$

Proof by Division into cases

$$p \vee q$$
$$p \to q$$
$$q \to r$$
$$\therefore r$$

Contradiction Rule

$$\sim p \to (contradiction)$$
$$\therefore p$$

1.4.4 Alternative method for determining validity

If an argument is *'invalid'* then there is a situation where all the premises are true but the conclusion is false.

Attempt to see whether this is possible. To do this, look for truth values which make all premises true yet the conclusion is false.

If such truth values can be found, then the argument is *invalid*

Summary of this method:

- Try to make all the premises true and the conclusion false
- If this can be done, then the argument is invalid
- On the other hand, if this is **impossible** to do, then the argument is valid

Checks for Validity

- Use a truth table
- Use rules of inference
- Attempt to find turht values that make all premises true but the conclusion false.

1.4.5 Predicates and domains

A predicate is a sentence that contains finitely many variables, and which becomes a statement if the variables are given specific values.

The domain of each variable in a predicate is the set of all possible values that may be assigned to it.

The truth set of a predicate P(x) is the set of all values in the domain that, when assigned to x, make P(x) a true statement.

Common Domains

- Integers: $\mathbb{Z}$ = [..., -3, -2, -1, 0, 1, 2, 3, ..]
- Positive integers: $\mathbb{Z}^+$ = [1, 2, 3, ...]
- Non-negative integers: $\mathbb{Z}^{non-neg}$ = [0, 1, 2, 3, ...]
- Natural numbers: $\mathbb{N}$ = [1, 2, 3, ...]
- Rational numbers: $\mathbb{Q}$ = [$\frac{a}{b}$ | a, b $\in \mathbb{Z} \wedge$ b $\neq 0$]
- Real numbers: $\mathbb{R}$ = entire number line

1.5 Quantifiers

1.5.1 Universal and Existental quantifiers

The Universal quantifier

The symbol '$\forall$' denotes *"for all"* and is called the **universal quantifier**

Let Q(x) be a predicate and **D** be the domain of x. The **universal statement**

$\forall$ x $\in$ **D**, Q(x)

is true if and only if Q(x) is true for every x in **D**. It is false if and only if Q(x) is false for at least one x in **D**

The Existental Quantifier

The symbol '$\exists$' denotes "there exists" and is called the **existential quantifier**

Let Q(x) be a predicate and **D** be the domain of x. The **existential statement**

$\exists$ x $\in$ **D** such that Q(x)

is true if and only if Q(x) is true for at least one x in **D**. It is false if and only if Q(x) is false for every x in **D**

1.5.2 Negation of Quantified Statements

Universal Statement:

$\forall$ x $\in$ **D**, Q(x)

The negation of this statement is logically equivalent to:

$\exists$ x $\in$ **D** such that $\sim$ Q(x)

Existential Statement:

$\exists$ x $\in$ **D** such that Q(x)

The negation of this statement is logically equivalent to:

$\forall$ x $\in$ **D**, $\sim$ Q(x)

Universal Conditional Statement

$\forall$ x $\in$ **D** if P(x) then Q(x)

The negation of this statment is logically equivalent to:

$\exists$ x $\in$ **D** such that $\sim$ if P(x) then Q(x)

which is;

$\exists$ x $\in$ **D** such that P(x) $\wedge$ $\sim$Q(x)

1.6 Multiple quantifiers

1.6.1 Intro to multiple quantifers

The predicate x $\leq$ y for real numbers x and y involves more than one variable.

Notation such as P(x,y) is used to denote such predicates.

Such predicates often appear in statments that involve more than one quantifier

In order to establish the truth of a statment of the form:

$\forall$ x $\in$ **D**, $\exists$ y $\in$ **D** such that P(x,y)

One must allow another to pick whatever element x $\in$ **D** they wish, and then must preceed with finding an element y $\in$ **E** which makes P(x,y) true.

In order to establish the truth of a statment of the form:

$\exists$ x $\in$ **D** such that $\forall$ y $\in$ **D**, P(x,y)

One must find one particular x $\in$ **D** which makes P(x,y) true no matter which y $\in$ **D** might be chosen for you.

1.6.2 Negation of statements with multiple quantifers

The statement:
$\forall$ x $\in$ **D**, $\exists$ y $\in$ **E** such that P(x,y)
Negates to:
$\exists$ x $\in$ **D** such that $\sim$ ($\exists$ y $\in$ **E** such that P(x,y))
Which is:
$\exists$ x $\in$ **D** such that $\forall$ y $\in$ **E** $\sim$ P(x,y)

The statement:
$\exists$ x $\in$ **D** such that $\forall$ y $\in$ **E**, P(x,y)
Negates to:
$\forall$ x $\in$ **D**, $\sim$ ($\forall$ y $\in$ **E**, P(x,y))
Which is:
$\forall$ x $\in$ **D**, $\exists$ y $\in$ **E** such that $\sim$ P(x,y))

2 Proofs and Number Theory

2.1 Proofs

2.1.1 Even and Odd

An integer 'n' is even if and only if 'n' is twice some integer.

- That is: n is even $\leftrightarrow \exists k \in \mathbb{Z}$ such that n = 2k

An integer 'n' is odd if and only if 'n' is twice some integer.

- That is: n is odd $\leftrightarrow \exists k \in \mathbb{Z}$ such that n = 2k + 1

2.1.2 Prime and Composite

An integer 'n' is prime if and only if n > 1 and for all positive integers 'r' and 's', if n = rs, then r = 1 or s = 1.

An integer 'n' is composite if and only if n > 1 and n = rs for some positive integers 'r' and 's' with r $\neq$ 1 and s $\neq$ 1

In symbols:

- n is prime $\leftrightarrow$ n > 1 $\wedge\forall$ r,s $\in \mathbb{Z}^+$, n = rs $\rightarrow$ (r=1 $\wedge$ s=1)
- n is composite $\leftrightarrow$ n > 1 $\wedge\exists$ r, s $\in \mathbb{Z}^+$ such that n = rs $\wedge$ r $\neq$ 1 $\wedge$ s $\neq$ 1
- Note: 1 is neither prime nor composite.

2.1.3 Direct proofs

Proving Existental Statements

To show $\exists$ x $\in$ **D** such that P(x) is true, it is enough to find one example of an element x in **D** for which P(x) is true.

Direct Proof of Universal Statements

One way to show that $\forall$ x $\in$ **D**, P(x) is true is by a direct proof.

1. Suppose x $\in$ **D**
2. Show that P(x) is true

Method of direct proof to show that $\forall$ x $\in$ **D** if P(x) then Q(x) is true:

1. Suppose x $\in$ **D** and P(x) is true
2. Show that the conclusion Q(x) is true using definitions, previously established results, and the rules for logical inference.

How to write a proof

- Write the theorem to be proved
- Clearly mark the beginning of the proof with the word *"Proof"*
- Use precise definitions for any mathematical terms
- Write the proof in complete sentences
- Give a reason for each assertion in your proof
- Make your proof self-contained
- Display equations and inequalities clearly
- Conclude by stating what it is you have proved

2.1.4 Other forms of proof

Disproof by Counterexample To show that $\forall$ x $\in$ **D** if P(x) then Q(x) is false, find a value of x $\in$ **D** for which P(x) is true and Q(x) is false.

Method of Proof by Contradiction

1. Assume that the statement is false
2. Show that this leads logically to a contradiction
    - So it is impossible that the statement is false

3. Conclude that the statement is true

Method of Proof by Contradiction to show that $\forall$ x $\in$ **D**, if P(x) then Q(x) is true:

1. Assume that the statement to be proved is false. Thus, the *negation* of the statement is true: $\exists$ x $\in$ **D** such that P(x) and $\sim$ Q(x)
2. Show that this assumption leads logically to a contradiction
3. Conclude that the statement to be proved is true.

Method of Proof by Contraposition

1. Express the statement to be proved in the form: $\forall$ x $\in$ **D**, if P(x) then Q(x)
2. Rewrite this statement in the contrapositive form: $\forall$ x $\in$ **D**, if $\sim$ Q(x) the $\sim$ P(x)
3. Prove the contrapositive by direct proof:
   - Suppose x $\in$ **D** and Q(x) is false
   - Show that P(x) is false

2.2 Types of numbers

2.2.1 Rational numbers

A real number is rational if and only if it can be expressed as a quotient of two integers with a non-zero denominator.

The set of all rational numbers is denoted by $\mathbb{Q}$

A real number that is not rational is irrational

r is rational $\leftrightarrow \exists$ a, b $\in \mathbb{Z}$ such that r = $\frac{a}{b}$ and b $\neq 0$

Fact: The decimal expansion of a rational number either repeats or terminates

Fact: The decimal expansion of an irrational number does not repeat and does not terminate

Theorem: For all rational numbers r and s where r < s, there exists another rational number q such that r < q < s

2.2.2 Divisibility

If n,d $\in \mathbb{Z}$, d $\neq 0$, then n is divisible by d if and only if there exists some k $\in \mathbb{Z}$ such that n = kd

Alternatively, we say

- n is a multiple of d
- d is a factor of n

- d is a divisor of n
- d divides n

The notation d|n is used to represent the predicate "d divides n"
If n is not divisible by d, we write d$\nmid$n
Theorem: Every integer n>1 can be written as a product of primes.
Proof: Suppose the theorem is false. Then there exists an integer n>1 that is not a product of primes.
Choose the smallest number *n*. Either n is prime or n is composite

- If n is prime; then n is trivially a product of primes
- If n is composite: then n = rs for some positive integers r and s, where r $\neq$ 1 and s $\neq$ 1. This implies that 1 < r < n and 1 < s < n

Because we chose n to be the smallest integer greater than 1 that is not a product of primes, both r and s (which are smaller than n) must be products of primes.
Therefore, n = rs is a product of primes also.
So, regardless of whether n is prime or composite, we find that n is a product of primes.
This contradicts our choice of n
Therefore, every integer n > 1 can be written as a product of primes.

2.2.3 Prime Factorisation

Given any integer n > 1, there exists

- A positive integer k
- Distinct primes p_1. p_2, ..., p_k
- Distinct primes e_1. e_2, ..., e_k such that
  n = $(p_1)^{(e_1)}(p_2)^{(e_2)}(p_3)^{(e_3)}...(p_k)^{(e_k)}$

and any other expression of n as a product of primes is identical to this, except perhaps for the order in which the terms are written

2.2.4 Floor and Ceiling

Given any x $\in \mathbb{R}$, the floor of x, denoted $\lfloor x \rfloor$, is the unique integer n such that n $\leq$ x < n+1
Given any x $\in \mathbb{R}$, the ceilling of x, denoted $\lceil x \rceil$, is the unique integer n such that n - 1 < x $\leq$ n+1

2.2.5 The quotient-remainder theorem

Given any integer n and a postiive integer d , there exists unique integers q and r such that

- n = dq + r and Q $\leq$ r $<$ d

For integers a and b, and a positive integer d, we say a is congruent to b modulo d and write

- a $\equiv$ b (mod d)

if and only if d | (a,b)

If a and b are not congruent modulo d, we write a /$\equiv$ b (mod d) [don't know how to represent this]

Facts:

- If n = dq + r, then n $\equiv$ r (mod d)
- n $\equiv$ 0 (mod d) if and only if d|n

2.3 Greatest common divisor

For integers $a,b \in \mathbb{Z}$, not both zero, the greatest common divisor of a and b, denoted gcd(a,b), is the integer d which satisfies the following two properties:

- d | a and d | b
- for all c $\in \mathbb{Z}$, if c | a and c | b then c $\leq$ d

Thus, d is the largest integer for which d | a and d | b

If gcd(a,b) = 1, then a and b have no common factors other than ± 1 and we call a and b coprime or relatively prime

What happens if a = b = 0?

For every d $\in \mathbb{Z}$, d satisfies d | 0 (d $\neq$ 0) since 0 = d.0. Thus, there is no greatest common divisor since there is no greatest integer.

However, if b $>$ 0, what is gcd(0,b)?

- d | 0 for all d $\in \mathbb{Z}$ (d $\neq$ 0)
- the greatest divisor of b is b

Thus, the greatest common divisor is 1

Fact: If b $>$ 0 then gcd(0,b) = b

Fact: If a and b are integers with b $\neq$ 0 and if q and r are integers such that:

$$a = bq + r \tag{1}$$

then gcd(a,b) = gcd(b,r)

Why?

- If d | a and d | b, then d | bq so d | (a - bq). Thus d | r
- If d | r and d | b, then d | bq so d | (bq+ r). Thus d | a

So the common divisors of a and b are the same as the common divisors of b and r.

2.3.1 The Euclidean Algorithm

To find gcd(a,b) where a,b $\in \mathbb{Z}$ and a $\geq$ b $>$ 0:

- Write a = bq + r, as in the quotient-remainder theorem
- If r=0, then terminate gcd(a,b) = b
- Otherwiste, replace (a,b) by (b,r) and repeat

Example: Find gcd(192, 132)

$$a = 192, b = 132, 192 = 132.1 + 60, gcd(192, 132) = gcd(132, 60) \quad (2)$$
$$a = 132, b = 60, 132 = 60.2 + 12, gcd(132, 60) = gcd(60, 12) \quad (3)$$
$$a = 60, b = 12, 60 = 12.5 + 0, gcd(60, 12) = gcd(12, 0) \quad (4)$$
$$Therefore, gcd(192, 132) = 12 \quad (5)$$

Could this process repeat forever? No. By the quotient-remainder theorem; 0 $\leq$ r $<$ b. Since we use the old value of r as the new value of b when we repeat, this means that r becomes strictly smaller on each repetition.

Therefore, we must eventually reach r=0 and terminate.

2.3.2 Lowest common multiple

For nonzero itnegers a,b $\in \mathbb{Z}$, the lowest common multiple of a and b is the smallest postive integer n for which a | n and b | n. We write this as lcm(a,b)

Fact: Suppose a,b $\in \mathbb{Z}$ where a $\leq$ b $>$ 0. Then gcd(a,b).lcm(a,b) = ab

2.4 Sequences

A sequence is an ordered list of elements. It can be finite or infinite.

Each individual element in a sequence is called a term. We often denote the terms of sequences by lower case letters with subscripts.

Note: The subscript of the initial term in a sequence does not need to be 1.

An explicit formula or general formula for a sequence is a rule showing how the value of a general term a_k depends on k.

Different notations are used to denote such a sequence, such as:

- $(2^k)_{k\leq 0}$
- $(2^k)_{k\leq 0}^{\infty}$

3 Logical Equivalences

Given any statement variables 'p', 'q' and 'r', a tautology '$\mathbf{t}$' and contradiction '$\mathbf{c}$', the following logical equivalences hold.

3.1 Commutative laws

- $p \wedge q \equiv q \wedge p$
- $p \vee q \equiv q \vee p$

3.2 Associative laws

- $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
- $(p \vee q) \vee r \equiv p \vee (q \vee r)$

3.3 Distributive laws

- $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
- $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

3.4 Identity laws

- $p \wedge \mathbf{t} \equiv p$
- $p \vee \mathbf{c} \equiv p$

3.5 Negation laws

- $p \vee \sim p \equiv \mathbf{t}$
- $p \wedge \sim p \equiv \mathbf{c}$

3.6 Double negative laws

- $\sim(\sim p) \equiv p$

3.7 Idempotent laws

- $p \vee p \equiv p$
- $p \wedge p \equiv p$

3.8 Universal bound laws

- $p \vee \mathbf{t} \equiv \mathbf{t}$
- $p \wedge \mathbf{c} \equiv \mathbf{c}$

3.9 De Morgan's laws

- $\sim(p \wedge q) \equiv \sim p \vee \sim q$
- $\sim(p \vee q) \equiv \sim p \wedge \sim q$

3.10 Absorption laws

- $p \vee (p \wedge q) \equiv p$
- $p \wedge (p \vee q) \equiv p$

3.11 Negations of t and c

- $\sim\mathbf{t} \equiv \mathbf{c}$
- $\sim\mathbf{c} \equiv \mathbf{t}$