MATH1064 Cheatsheet

Abyan Majid

August 30, 2023

---

1 Logic, inference, and proof

1.1 Truth tables

p	q	**NOT** p $\neg p$	p **AND** q $p \wedge q$	p **OR** q $p \vee q$	p **XOR** q $p \oplus q$	**IF** p **THEN** q $p \rightarrow q$	q **IF AND ONLY IF** p $p \iff q$
T	T	F	T	T	F	T	T
T	F	F	F	T	T	F	F
F	T	T	F	T	T	T	F
F	F	T	F	F	F	T	T

1.2 Logical equivalences

1.2.1 Logical laws

Logical equivalence	**Name of law**
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	Distributive laws
$p \wedge q \equiv q \wedge p$ $p \vee q \equiv q \vee p$	Commutative laws
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ $(p \vee q) \vee r \equiv p \vee (q \vee r)$	Associative laws
$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	Identity laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Universal bound laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws
$\neg(\neg p) \equiv p$	Double negation law
$p \wedge p \equiv p$ $p \vee p \equiv p$	Idempotent laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws

1.2.2 Equivalences for conditionals and biconditionals

Logical equivalence	**Description**
$p \to q \equiv \neg p \vee q$	Expressing $p \to$ as $\neg p \vee$
$p \iff q \equiv (p \to q) \wedge (q \to p)$	Expressing $\iff$ as a conjunction of conditionals

1.2.3 Equivalences for quantifiers

Logical equivalence	**Description**
$\forall x \in D, P(x) \equiv P(x_1) \wedge P(x_2) \wedge ... \wedge P(x_n)$	Expressing $\forall$ as a conjunction of predicates
$\exists x \in D : P(x) \equiv P(x_1) \vee P(x_2) \vee ... \vee P(x_n)$	Expressing $\exists$ as a disjunction of predicates

1.3 Contrapositive, converse, and inverse of conditional statements

Given a conditional statement $p \to q$	
Contrapositive	$\neg q \to \neg p$
Converse	$q \to p$
Inverse	$\neg p \to \neg q$

1.4 Negation of quantifiers

Given	Negation
$\forall x \in D, P(x)$	$\exists x \in D : \neg P(x)$
$\exists x \in D : P(x)$	$\forall x \in D, \neg P(x)$

1.5 Rules of inference

Rule of inference	**Name**
$\begin{array}{c} p \\ \underline{p \to q} \\ \therefore q \end{array}$	Modus ponens
$\begin{array}{c} \neg q \\ \underline{p \to q} \\ \therefore \neg p \end{array}$	Modus tollens
$\begin{array}{c} p \to q \\ \underline{q \to r} \\ \therefore p \to r \end{array}$	Hypothetical syllogism
$\begin{array}{c} p \vee q \\ \underline{\neg p} \\ \therefore q \end{array}$	Disjunctive syllogism
$\begin{array}{c} \underline{p} \\ \therefore p \vee q \end{array}$	Addition/generalization
$\begin{array}{c} \underline{p \wedge q} \\ \therefore p \end{array}$	Simplification/specialisation
$\begin{array}{c} p \\ \underline{q} \\ \therefore p \wedge q \end{array}$	Conjunction
$\begin{array}{c} p \vee q \\ \neg p \vee r \end{array}$	Resolution

1.6 Rules of inference for quantified statements

Rule of inference	Name
$\dfrac{\forall x P(x)}{\therefore P(c)}$	Universal instantiation
$\dfrac{P(c) \text{ for arbitrary } c}{\therefore \forall x P(x)}$	Universal generalisation
$\dfrac{\exists x P(x)}{\therefore P(c) \text{ for some } c}$	Existential instantiation
$\dfrac{P(c) \text{ for some } c}{\therefore \exists x P(x)}$	Existential generalisation

1.7 Proof methods

Name of proof	**Step-by-step procedure**	**Effective use case**
Direct proof	To prove $p \to q$: 1. assume p is true 2. show that q must also be true otherwise $p \to q$ is false since $\mathbf{T} \to \mathbf{F} \equiv \mathbf{F}$	When given a statement in the form $p \to q$
Proof by contraposition	Since $p \to q \equiv \neg q \to \neg p$, to prove $p \to q$: 1. assume $\neg q$ is true 2. show that $\neg p$ must also be true otherwise $\neg q \to \neg p$ is false since $\mathbf{T} \to \mathbf{F} \equiv \mathbf{F}$, and therefore $p \to q$ is false.	When given a statement in the form $p \to q$, and direct proof failed.
Proof by contradiction	To prove p, 1. assume $\neg p$ is true 2. show that $\neg p$ leads to a contradiction, i.e. $\neg p \to (r \wedge \neg r)$. Otherwise, p is true.	When given a statement in the form p
Disproof by counterexample	To disprove $\forall x \in D, P(x)$, find one example for which $P(x)$ is false.	When given state- -ments with universal quantifiers.
Proof by cases	To prove $\forall x \in D, P(x)$, 1. identify all cases for which the truthness/falsity of P(x) may vary. 2. make assumptions WLOG where necessary 3. show that all cases prove $P(x)$ true/false.	When it appears that you can prove one example and and every other example will follow.

1.7.1 Without loss of generality (WLOG)

Without loss of generality (WLOG) is the act of making a simplifying assumption along the lines of: "if this simple case is true, then trivially every other cases must be true".

2 Sets, functions, sequences, sums

2.1 Set theory

2.1.1 Union, intersection, difference, complement, subset

Name	**Set operation**	**Description**
Union	$A \cup B$	All elements that are in A or B or both
Intersection	$A \cap B$	All elements that are both in A and B
Difference	$A \setminus B$	All elements that are in A but not in B
Complement	$\overline{A}$	All elements in the universal set that are not in A
Subset	$A \subseteq B$	A is a subset of B; every element in A is also in B
Proper subset	$A \subsetneq B$	A is a subset of B and $A \neq B$.

2.1.2 Set identities and their logic counterparts

Set	**Logic**
$\cap$ (intersection)	$\wedge$ (and)
$\cup$ (union)	$\vee$ (or)
$\overline{A}$ (complement)	$\neg$ (not)
U (universal set)	**T** (tautology)
$\emptyset$ (empty set)	**F** (contradiction)

2.1.3 Cardinality, power set, and cartesian product of sets

Name	**Operation**	**Description**	**Given** $A = \{p, q\}$**,** $B = \{r, s\}$
Cardinality	$\lvert A \rvert$	Number of elements in A	$\lvert A \rvert = 2$
Power set (Size of set $= 2^n$)	$\mathcal{P}(A)$	Set of all subsets of A including the empty set	$\mathcal{P}(A) = \{\emptyset, \{p\}, \{q\}, \{p, q\}\}$
Cartesian product (Size of set $= \lvert A \rvert \cdot \lvert B \rvert$)	$A \times B$	Set of all ordered n-tuples from A and B	$A \times B = \{(p, r), (p, s), (q, r), (q, s)\}$

2.1.4 Proof methods for set equivalences

To prove $A = B$, show that A $\subseteq$ B and B $\subseteq$ A	
Method	**Step-by-step procedure**
Element method	To prove $A \subseteq B$, 1. let $x \in A$ 2. construct worded proof with set operations to arrive at $x \in B$
Logical equivalences	To prove $A \subseteq B$, 1. let $x \in A$ 2. rewrite set operators with their logical counterparts 3. derive $x \in B$ from $x \in A$ using logical equivalences

2.2 Functions

2.2.1 Domain, codomain, preimage, image, range of functions

Given $f : X \to Y$		Given $f(x) = y$	
Terminology	**Description**	**Terminology**	**Description**
Domain (X)	All possible inputs for f	Preimage (x)	$x \in X$ that is mapped to some $y \in Y$ by f
Codomain (Y)	All possible outputs for f	Image (y)	$y \in Y$ to which some $x \in X$ is mapped by f

2.2.2 Injective, surjective, bijective, and composite functions

Function type	Definition
Injective (one-to-one)	A function $f : X \to Y$ where $\forall x \in X$, x is assigned a different $y \in Y$, and $\lvert X\rvert \leq \lvert Y\rvert$.
Surjective (onto)	A function $f : X \to Y$ where all $\forall y \in Y$, y is an image of some $x \in X$, and $\lvert X\rvert \geq \lvert Y\rvert$.
Bijective (one-to-one correspondence)	A function that is both injective and surjective, where $\lvert X\rvert = \lvert Y\rvert$
Composite	A function $(f \circ g)(a) = f(g(a))$ where a function f takes another function g as input.

2.2.3 Proving injection, surjection, and non-existent functions

What to prove	How to prove
$f : X \to Y$ is injective	1) If a graph of f is given or derivable, commit horizontal line test 2) Alternatively, show that if $f(x_1) = f(x_2)$ for arbitrary $x_1, x_2 \in X$ with $x_1 \neq x_2$, then $x_1 = x_2$.
$f : X \to Y$ is NOT injective	Show that $\exists x_1, x_2 \in X$ such that $x_1 \neq x_2$ and $f(x_1) = f(x_2)$
$f : X \to Y$ is surjective	Show that $\forall y \in \mathbb{Z}, \exists x \in \mathbb{Z}$ such that $f(x) = y$
$f : X \to Y$ is NOT surjective	Show that $\exists y \in Y$ such that $\forall x \in X$, $f(x) \neq y$
$f : X \to Y$ is not a function	1) If a graph of f is given or derivable, commit vertical line test if there exists a vertical line that intersects the graph more than once, then f is not a function. 2) If the expression for f is given, make y the subject and prove algebraically that there are more than one value for y.

2.3 Sequences and sums

2.3.1 Arithmetic and geometric sequences, and recurrence

Name of sequence	Definition	n-th Term	Series
Arithmetic sequence	$\{a, a+d, a+2d, ..., a+nd\}$, where a is the initial term and d is difference	$a_n = a_1 + (n-1)d$	$S_n = n(\frac{a_1 + a_n}{2}))$
Geometric sequence	$\{a, ar, ar^2, ..., ar^n\}$, where a is the initial term and r is common ratio	$a_n = ar^{n-1}$	$S_n = a_1(\frac{1-r^n}{1-r})$

2.3.2 Reccurrence relation

Recurrence relation	
Notation	**Definition**
$a_n = \{a_0, a_1, a_2, ..., a_{n-1}\}$	equation that expresses every term in some sequence $\{a\}$ in terms of one or more of the previous terms in the sequence

2.3.3 Fibonacci and factorials sequences

Name of sequence	**Definition**
Fibonacci sequence	a sequence $\{f_0, f_1, f_2\}$ defined by initial conditions $f_0 = 0$, $f_1 = 1$ and the recurrence relation $f_n = f_{n-1} + f_{n-2}$ for $n = 2, 3, 4, ...$
Factorials sequence	$(n!)_{n\geq 0} = \{1, 1, 2, 6, 24, 120, ...\}$, or defined recursively as $0! = 1$, $n! = (n-1)! \times n$ for $n \geq 1$

2.3.4 Summation notation

To represent the sum of some sequence $a_m + a_{m+1} + ... + a_n$, we write: $\sum_{i=m}^{n} a_i$

2.3.5 Summation definitions

Property	**Definition**
Addition/subtraction over the same range	$\displaystyle\sum_{i=m}^{n} a_i \pm \sum_{i=m}^{n} b_i = \sum_{i=m}^{n}(a_i \pm b_i)$
Taking out a common factor	$\displaystyle\sum_{i=m}^{n} ca_i = c\sum_{i=m}^{n} a_i$
Combining consecutive indices	$\displaystyle\sum_{i=p}^{q} a_i + \sum_{i=q+1}^{r} a_i = \sum_{i=p}^{r} a$ if $p \leq q \leq r$
Index shift	$\displaystyle\sum_{i=m}^{n} a_i = \sum_{i=m+p}^{n+p} a_{i-p} = \sum_{i=m-q}^{n-q} a_{i+q}$
Telescoping sums	$\displaystyle\sum_{i\,=\,m}^{n} (a_i - a_{i+1}) = a_m - a_{n+1}$ if $m \leq n$

3 Number theory

3.1 Divisibility and modular arithmetic

3.1.1 Addition, multiplication, and transitivity theorems of divisibility

Theorem	**Definition**
Addition	If $a\|b$ and $a\|c$, then $a\|(b+c)$
Multiplication	If $a\|b$, then $a\|bc$ for all $c \in \mathbb{Z}$
Transitivity	If $a\|b$ and $b\|c$, then $a\|c$

3.1.2 Quotient-Remainder theorem

Quotient-Remainder Theorem
Given integer $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$, then there exists Two unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$

3.1.3 Expressions for quotient and remainder

Expressions for quotient (q) and remainder (r)
$q = a\ \mathbf{div}\ d = \lfloor \frac{a}{d} \rfloor$ $r = a\ \mathbf{mod}\ d = a - (d \times \lfloor \frac{a}{d} \rfloor)$

3.1.4 Lemma: bounds for divisors

Bounds for divisors
Let $n, d \in \mathbb{Z}$. If $\|n\| \geq 1$ and $d\|n$, then $0 < \|d\| \leq \|n\|$

3.1.5 Congruence definition

Congruence
$a \equiv b\ (\mathbf{mod}\ m)$ denotes that a is congruent to b $(\mathbf{mod}\ m)$ if and only if $m\|(a-b)$

3.1.6 Congruence theorems

Theorem 1
If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then a and b are congruent modulo m if and only if $\exists k \in \mathbb{Z}$ such that $a = b + km$

Theorem 2
Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, if $a \equiv b\ (\mathbf{mod}\ m)$ and $c \equiv d\ (\mathbf{mod}\ m)$, then $a + c \equiv b + d\ (\mathbf{mod}\ m)$ and $ac \equiv bd\ (\mathbf{mod}\ m)$

4 Primes, GCD, and LCM

4.1 Definitions and theorems for primes

Name	**Definition**
Prime number	Given $p \in \mathbb{Z}$ with $p > 1$, p is prime if the only positive factors of p are 1 and p.
Fundamental theorem of arithmetic	$\forall x \in \mathbb{Z}$ where $x > 1$, x can be written uniquely as a prime, or as a product of 2 or more primes where the prime factors are written in order of nondecreasing size.
Composite integer	$k \in \mathbb{Z}^+$ is a composite integer if $\exists a, b \in \mathbb{Z}^+$ where $a < k$ and $b < k$, such that $k = ab$.
Relatively prime	Let $a, b \in \mathbb{Z}$, a and b are realtively prime if $\gcd(a, b) = 1$
Pairwise relatively prime	$a_1, a_2, ..., a_n \in \mathbb{Z}$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i \leq j \leq n$

4.2 GCD and LCM definitions

Name	**Definition**
Greatest Common Divisor	Let $a, b \in \mathbb{Z}$ where $a \neq 0$ and $b \neq 0$. The GCD of a and b, denoted $\gcd(a, b)$ is d such that $d\|a$ and $d\|b$
Least Common Multiple	The LCM of a and b, denoted $\operatorname{lcm}(a, b)$, is the smallest $l \in \mathbb{Z}^+$ such that $a\|k$ abd $b\|k$
Relationship between GCD and LCM of $a, b \in \mathbb{Z}$	$ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$

4.3 Finding GCD and LCM via prime factorization

Suppose the prime factorization of $a, b \in \mathbb{Z}$ are: $a = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_n^{a_n}$ $b = p_1^{b_1} \cdot p_2^{b_2} \cdot ... \cdot p_n^{b_n}$	
What to find	**How**
GCD	$\gcd(a, b) = (P_1^{\min(a_1,b_1)})(P_2^{\min(a_2,b_2)})...(P_n^{\min(a_n,b_n)})$
LCM	$\text{lcm}(a, b) = (P_1^{\max(a_1,b_1)})(P_2^{\max(a_2,b_2)})...(P_n^{\max(a_n,b_n)})$

4.4 Verifying prime using trial division

Trial divison
Given $a \in \mathbb{Z}$, a is prime, if for all primes $k \leq \sqrt{a}$, $k \mid a$.