Midterm 1 Précis

MATH 55 Spring 2025

Instructor: James Demmel

---

1 Logic and Proofs

1. Proposition

   (a) Logical Propositions, Compound Operations, Conditionals and Biconditionals, Truth Tables

p	q	$\neg p$	$p \vee q$	$p \wedge q$	$p \oplus q$	$p \to q$	$p \leftrightarrow q$
T	T	F	T	T	F	T	T
T	F	F	T	F	T	F	F
F	T	T	T	F	T	T	F
F	F	T	F	F	F	T	T

   (b) Tautologies and Contradictions

p	$p \vee \neg p$	$p \wedge \neg p$
T	T	F
F	T	F.

   (c) Logical Equivalence Rules

Equivalence	Name
$p \wedge T \equiv p$	Identity laws
$p \vee F \equiv p$	
$p \vee T \equiv T$	Domination laws
$p \wedge F \equiv F$	
$p \vee p \equiv p$	Idempotent laws
$p \wedge p \equiv p$	
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$	Commutative laws
$p \wedge q \wedge q \vee p$	Commutative laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$	Associative laws
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	Distributive laws
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	
$\neg(p \wedge q) \equiv \neg p \vee \neg q$	De Morgan's laws
$\neg(p \vee q) \equiv \neg p \wedge \neg q$	
$p \vee (p \wedge q) \equiv p$	Absorption laws
$p \wedge (p \vee q) \equiv p$	
$p \vee \neg p \equiv T$	Negation laws
$p \wedge \neg p \equiv F$	

2. Predicates and Quantifiers

   (a) quantifiers table

Statement	True when...	False when...
$\forall x P(x)$	$P(x)$ is true for every x.	There is an x for which $P(x)$ is false.
$\exists x P(x)$	There is an x for which $P(x)$ is true.	$P(x)$ is false for every x.

   (b) De Morgan's Laws for Quantifiers

Negation	Equivalent	Negation true when...	Negation false when...
$\neg\exists x P(x)$	$\forall x \neg P(x)$	For every x, $P(x)$ is false.	There is an x for which $P(x)$ is true.
$\neg\forall x P(x)$	$\exists x \neg P(x)$	There is an x for which $P(x)$ is false.	$P(x)$ is true for every x.

   (c) Quantifications of Two Variables.

Statement	True when...	False when...
$\forall x \forall y P(x,y)$	$P(x,y)$ true for every pair x, y.	There is a pair x, y for which $P(x,y)$ is false.
$\forall y \forall x P(x,y)$		
$\forall x \exists y P(x,y)$	For every x there is a y for which $P(x,y)$ is true.	There is an x such that $P(x,y)$ is false for every y.
$\exists x \forall y P(x,y)$	There is an x for which $P(x,y)$ is true for every y.	For every x there is a y for which $P(x,y)$ is false.
$\exists x \exists y P(x,y)$	There is a pair x, y for which $P(x,y)$ is true.	$P(x,y)$ is false for every pair x, y.

3. Rules of Inference

   (a) Rules of Inference Table

Tautology	Name (not important)
$(p \wedge (p \to q)) \to q$	Modus ponens
$(\neg q \wedge (p \to q) \to \neg p$	Modus tollens
$((p \to q) \wedge (q \to r)) \to (p \to r)$	Hypothetical syllogism
$((p \vee q) \wedge \neg p) \to q$	Disjunctive syllogism
$p \to (p \vee q)$	Addition
$(p \wedge q) \to p$	Simplification
$((p) \wedge (q)) \to (p \wedge q)$	Conjunction
$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r)$	Resolution

   (b) Rules of Inference for Quantified Statements.

Rule of Inference	Name
$\forall x P(x) \implies P(c)$ for some element c	Universal instantiation
$P(c)$ for an arbitrary $c \implies \forall x P(x)$	Universal generalization
$\exists x P(x) \implies P(c)$ for some element c	Existential instantiation
$P(c)$ for some element $c \implies \exists x P(x)$	Existential generalization.

4. Proof Strategies: direct, contraposition, contradiction.

2 Sets

1. Set Definitions

Dfn (Set)**.** Collection of unordered distinct objects A. Elements $a \in A$ are members of the set.

Dfn (Subset)**.** $A \subseteq B$ iff $a \in A \implies a \in B$. $A \subset B$ is a proper subset of A if $A \subseteq B$, but $\exists b \in B$ s.t. $b \notin A$.

Set	Elements	Name
$\emptyset$	-	Empty set
$\mathbb{N}$	$\{0, 1, 2, 3, ...\}$	Natural numbers
$\mathbb{Z}$	$\{..., -2, -1, 0, 1, 2, ...\}$	Integers
$\mathbb{Z}^+$	$\{1, 2, 3, ...\}$	Positive integers
$\mathbb{Q}$	$\{r \mid r = p/q, p, q \in \mathbb{Z}\}$	Rational numbers
$\mathbb{R}$	-	Real numbers
$\mathbb{R}^+$	$\{r \in \mathbb{R} \mid r > 0\}$	Positive real numbers
$\mathbb{C}$	$\{a + bi \mid a, b \in \mathbb{R}\}$	Complex numbers

$$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$$
$$(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$$
$$[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$$
$$(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$$

2. Set Operations

Dfn (Set Operations)**.**

- $\mathcal{P}(S) = \{U \mid U \subseteq S\}$
- $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$
- $A \cup B = \{x \mid x \in A \vee x \in B\}$
- $A \cap B = \{x \mid x \in A \wedge x \in B\}$
- $\overline{A} = \{x \mid x \notin A\}$
- $A \setminus B = A - B = \{x \mid x \in A \wedge x \notin B\}$

3. Set Laws

Identity	Name
$A \cap U = A$ $A \cup = A$	Identity laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{\overline{A}} = A$	Complementation laws
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws

3 Functions

Dfn (Function)**.** $f : X \to Y$ is an assigment of an element of y to each element of x, $f(x) = y$. X domain, Y codomain. Range/Image $= f(X)$. Note: if $f : X \to Y$, then at most one element of y can be assigned to each x. If $f_1, f_2 : A \to \mathbb{R}$, then

$$(f_1 + f_2)(x) = f_1(x) + f_2(x), \quad (f_1 f_2)(x) = f_1(x) f_2(x).$$

Dfn (Properties)**.**

- **(1-1):** $f(x) = f(y) \implies x = y$.
- **(onto):** $\forall y \in Y, \exists x$ s.t. $f(x) = y$. I.e. $f(X) = Y$.
- **(bijection):** 1-1 and onto.
- **(composition):** $f : X \to Y$, $g : Y \to Z$, then $g \circ f : X \to Z$, $g \circ f(x) = g(f(x))$.
- **(preimage):** $f : X \to Y$, $S \subseteq Y$. Then $f^{-1}(S) = \{x \in X \mid f(x) \in S\}$.
- **(inverse):** $f : X \to Y$ a bijection. Then $f^{-1} : Y \to X$ s.t. $f \circ f^{-1} = f^{-1} \circ f =$ identity map $x \mapsto x$.

4 Counting and Cardinality

Dfn (Cardinality). $|A|$ = number of elements in A.

- **(finite):** $|A| < \infty$
- **(countable):** $\exists f : A \to \mathbb{N}$ bijection $|A| = \aleph_0$
- **(uncountable):** A not countable.

Prop (Union/intersection). A, B countable then

- $A \cup B$ countable
- $A \cap B$ countable

Prop (Countable union). A countable, $\{B_a\}_{a \in A}$, B_a $\forall a \in A$, then $\cup_{a \in A} B_a$ countable.

Prop (Cartesian product). A, B countable $\implies$ $A \times B$ countable.

5 Divisibility and Modular Arithmetic

Dfn (Divisibility). $a, b \in \mathbb{Z}$. $a|b$ iff $\exists n \in \mathbb{Z}$ s.t. $b = an$.

- $a|b$, $a|c \implies a|(b+c)$
- $a|b \implies a|bc$ $\forall c \in \mathbb{Z}$
- $a|b \wedge b|c \implies a|c$

Thm (Division Algorithm). $a, d \in \mathbb{Z}$, $d > 0$. $\exists! q, r \in \mathbb{Z}$ s.t. $0 \leq r < d$ and $a = dq + r$.

$$q = \textbf{ div } d, \quad r = a \textbf{ mod } d$$

Thm (Laws of Modular Arithmetic).

- $(a+b)$ **mod** $m = ((a$ **mod** $m) + (b$ **mod** $m))$ **mod** m
- ab **mod** $m = (a$ **mod** $m)(b$ **mod** $m)$ **mod** m

Thm (Base Representation). $b, n \in \mathbb{Z}^+$, $b > 1$. $\exists!$ representation $n = a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0$ where $k \geq 0$ and $\forall i = 1, ..., k$, $0 \leq a_i < b$, $a_k > 0$.

Dfn (Congruence). $a, b, m \in \mathbb{Z}$, $m > 0$. Then $a \equiv b \pmod{m}$ iff a **mod** $m = a$**mod** m.

Dfn (Prime). $p \in \mathbb{Z}^+ \setminus \{1\}$ **prime** if the only positive factors of p are 1 and p. Otherwise **composite.**

Thm (Fundamental Theorem of Arithmetic). $a \in \mathbb{Z}^+$. Then $\exists! p_1, ..., p_k$ primes and $n_1, ..., n_k \in \mathbb{N}$ such that $a = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$.

Dfn (gcd and lcm). $a, b \in \mathbb{Z}^+$, $b \neq 0$.

- $g := \gcd(a, b)$ satisfies $g|a \wedge g|b$ and g maximal.
- a, b **relatively prime** iff $\gcd(a, b) = 1$.
- $l := \text{lcm}(a, b)$ satisfies $a|l \wedge b|l$ and l minimal
- $a \cdot b = \text{lcm}(a, b) \cdot \gcd(a, b)$

Thm (Bezout's Lemma). $a, b \in \mathbb{Z}^+$, $b \neq 0$. Then $\exists s, t \in \mathbb{Z}$ such that $sa + tb = \gcd(a, b)$.

Thm (Euclidean Algorithm). $a, b \in \mathbb{Z}^+$, $b \neq 0$. Set $b_0 = b$, $a_0 = a$.

```
x := a
y := b
while y \neq 0:
    r := x mod y
    x := y
    y := r
return x
```

6 Congruence

Dfn (Congruence). $ax \equiv b \pmod{m}$

Dfn (Multiplicative inverse). $\bar{a}$ inverse of a modulo m iff $\bar{a}a \equiv 1 \pmod{m}$. Unique up to multiples of m.

Prop (Euclidean gives inverses).

```
1) Run Euclidean alg on (a,m) and get as+tm=1
2) mod m to get as+tm \equiv 1 mod m
3) Observe as \equiv 1 mod m implies s=\bar{a}
```

Thm (Chinese Remainder Theorem). $m_1, ..., m_n$ relatively prime and > 1, $a_1, ..., a_n \in \mathbb{Z}$. $\exists!$ solution x modulo $m = m_1 ... m_n$ to the system

$$\{x \equiv a_i \pmod{m_i}\}_{i=1,...,n}.$$

Thm (Chinese Remainder Theorem Algorithm).

```
m := m_1m_2...m_n
for all k = 1, ..., n:
    M_k := m/m_k
    y_k := inverse(M_k mod m_k)
x := a_1M_1y_1 +...+ a_nM_ny_n
```

Thm (Fermat's Little Theorem). p prime, $a \in \mathbb{Z}$ and $p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}$.