FINAL Study Guide

Andrew Reed
Discrete Final

May 8, 2018

Contents

1 The Foundations: Logic and Proofs

1.1 Propositional Logic

Examples of a proposition:
$p(x) = x$ is a cat.
$q(x) = x$ has fur.

1. Negation, $\neg p(x)$, changing the statement to x is not a cat
2. Conjunction, $p(x) \wedge q(x)$, changing the statement to say x is a cat and it has fur.
3. Disjunction, $p(x) \vee q(x)$, changing the statement to say x is a cat and it does not have fur.
4. Exclusive Or, $p(x) \oplus q(x)$, where the statement is true only when exactly one of $p(x)$ or $q(x)$ is true, otherwise the statement is false.
5. Conditional Statement, $p(x) \rightarrow q(x)$, where the statement is read "If p, then q" the statement is false when p is true and q is false, otherwise the statement is true.
6. Bi-Conditional Statement, $p(x) \leftrightarrow q(x)$, where the statement is true if the values of p and q match. The statement is read as any of the following;
   (a) "p if and only if q"
   (b) "p is necessary and sufficient for q"
   (c) "if p then q, and conversely"
   (d) "p iff q"
7. Converse, Contrapositive, and Inverse
   Given $p \rightarrow q$;
   (a) Converse: $q \rightarrow p$
   (b) Contrapositive: $\neg q \rightarrow \neg p$
   (c) Inverse: $\neg p \rightarrow \neg q$

Definitions

1. Hypothesis - p is considered the hypothesis in the statement $p(x) \rightarrow q(x)$.
2. Conclusion- q is considered the conclusion in the statement $p(x) \rightarrow q(x)$.
3. Bi-Implications - Another way to express "Bi-Conditional statements"

1.2 Propositional Equivalences

1. Logically Equivalent, $p(x) \equiv q(x)$, when two statements share the same truth values then the statement is said to be logically equivalent.

2. Identity Laws
$$p(x) \wedge T \equiv p(x)$$
$$p(x) \vee F \equiv p(x)$$

3. Domination Laws
$$p(x) \vee T \equiv T$$
$$p(x) \wedge F \equiv F$$

4. Idempotent Laws
$$p(x) \vee p(x) \equiv p(x)$$
$$p(x) \wedge p(x) \equiv p(x)$$

5. Double Negation Law
$$\neg(\neg p(x)) \equiv p(x)$$

6. Commutative Laws
$$p(x) \vee q(x) \equiv q(x) \vee p(x)$$
$$p(x) \wedge q(x) \equiv q(x) \wedge p(x)$$

7. Associative Laws
$$(p(x) \vee q(x)) \vee r(x) \equiv p(x) \vee (q(x) \vee r(x))$$
$$(p(x) \wedge q(x)) \wedge r(x) \equiv p(x) \wedge (q(x) \wedge r(x))$$

8. Distributive Laws
$$p(x) \vee (q(x) \wedge r(x)) \equiv (p(x) \vee q(x)) \wedge (p(x) \vee r(x))$$
$$p(x) \wedge (q(x) \vee r(x)) \equiv (p(x) \wedge q(x)) \vee (p(x) \wedge r(x))$$

9. De Morgan's Laws
$$\neg\,(p(x) \wedge q(x)) \equiv \neg p(x) \vee \neg q(x)$$
$$\neg\,(p(x) \vee q(x)) \equiv \neg p(x) \wedge \neg q(x)$$

10. Absorption Laws
$$p(x) \vee (p(x) \wedge q(x)) \equiv p(x)$$
$$p(x) \wedge (p(x) \vee q(x)) \equiv p(x)$$

11. Negation Laws
$$p(x) \vee \neg p(x) \equiv T$$
$$p(x) \wedge \neg p(x) \equiv F$$

Definitions

1. Tautology - When all cases in the statement are determined to be true, it is said to be a tautology.

2. Contradiction- When all cases in the statement are determined to be false, it is said to be a contradiction.

3. Contingency - When the statement is neither a tautology, nor a contradiction then it is said to be a contingency.

1.3 Predicates and Quantifiers

1. Universal Quantification, $\forall p(x)$ read as, "For all x, $p(x)$."

2. Existential Quantification, $\exists p(x)$ read as, "There exists an element x, that $p(x)$."

3. De Morgan's Laws for Quantifiers:

$$\neg\forall p(x) \equiv \exists\neg p(x)$$

$$\neg\exists p(x) \equiv \forall\neg p(x)$$

Definitions

1. Quantification - Used to express the extent that a predicate is true. In English, the words; all, some, many, none, and few are used in quantifications.

2. Counterexample - When there is a value, x in which $\forall p(x)$ is false, then that value of x is called a counterexample of $\forall p(x)$.

1.4 Rules of Inference (ROI)

Modus Ponens

$$\begin{array}{c} p \\ p \to q \\ \hline \therefore q \end{array}$$

Modus Tollens

$$\begin{array}{c} \neg q \\ p \to q \\ \hline \therefore \neg p \end{array}$$

Hypothetical Syllogism

$$\begin{array}{c} p \to q \\ q \to r \\ \hline \therefore p \to r \end{array}$$

Disjunctive Syllogism

$$\begin{array}{c} p \lor q \\ \neg p \\ \hline \therefore q \end{array}$$

Addition

$$\begin{array}{c} p \\ \hline \therefore p \lor q \end{array}$$

Simplification

$$\begin{array}{c} p \land q \\ \hline \therefore p \end{array}$$

Conjunction

$$\begin{array}{c} p \\ q \\ \hline \therefore p \land q \end{array}$$

Universal Instantiation

$$\begin{array}{c} \forall p(x) \\ \hline \therefore p(c) \end{array}$$

Universal Generalization

$$\begin{array}{c} p(c) \text{ for an arbitrary c} \\ \hline \therefore \forall p(x) \end{array}$$

Existential Instantiation

$$\begin{array}{c} \exists p(x) \\ \hline \therefore p(c) \text{ for some element c} \end{array}$$

Existential Generalization

$$\begin{array}{c} p(c) \text{ for some element c} \\ \hline \therefore \exists p(x) \end{array}$$

Definitions

1. Argument - Sequence of propositions.
2. Premises - All propositions in the argument with the exclusion of the conclusion
3. Conclusion - The final proposition in the argument.
4. Argument Form - A sequence of compound propositions involving propositional variables.
5. Valid - A form that makes it impossible for the premises to be true and the conclusion nevertheless to be false.

1.5 Proofs

1. direct proof:

   Directly prove that if n is an odd integer then n^2 is also an odd integer.

   PROOF ($\rightarrow$):

   An odd number is denoted by the equation, $2k+1$

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

   $2(2k^2 + 2) + 1$, is another form of 2k + 1.

   Therefore, if n is an odd integer then n^2 is also an odd integer.

2. Proofs by Contradiction:

Definitions

1. Theorem - A statement that can be shown to be true.
2. Proof - A demonstration that a theorem is true.
3. Axioms (or postulates) - Statements we assume to be true.
4. Lemma - A less important theorem that is helpful in the proof of other results.
5. Corollary - A theorem that can be established directly from a theorem that has been proved.
6. Conjecture - A statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert. When a proof of a conjecture is found, the conjecture becomes a theorem.

2 Sets, Functions, Sequences, Sums, and Matrices

2.1 Sets

A set is an unordered collection of objects, called elements or members of the set.
We write $a \in A$ to denote that a is an element of the set A.
We write $a \notin A$ denotes that a is not an element of the set A

Well known sets include;
$\mathbb{N} = \{0, 1, 2, 3, ...\}$, the set of natural numbers
$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$, the set of integers
$\mathbb{Z}+ = \{1, 2, 3, ...\}$, the set of positive integers
$Q = \{p/q|p \in \mathbb{Z},\ q \in \mathbb{Z},\ and\ q \neq 0\}$, the set of rational numbers R, the set of real numbers
$\mathbb{R}+$, the set of positive real numbers
$\mathbb{C}$, the set of complex numbers.
Ω, the universal set

Showing that A is a Subset of B To show that $A \subseteq B$, show that if x belongs to A then x also belongs to B.

Showing that A is Not a Subset of B To show that $A \nsubseteq B$, find a single x ∈ A such that x ∉ B.

Showing Two Sets are Equal To show that two sets A and B are equal, show that $A \subseteq B$ and $B \subseteq A$.

Every set (S) includes the following two sets;

$$S \subseteq S \qquad AND \qquad \emptyset \subseteq S$$

A set (S) is said to be a finite set when it has exactly n distinct elements and n is said to be the cardinality of S, denoted as $|S|$

The Power Set of a set (S) is the set of all subsets of S. It is denoted as $\wp(S)$

2.2 Set Operations

Let A and B be sets. The Cartesian product of A and B, denoted as $A \times B$, is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$

Let A and B be sets. The union of the sets A and B, denoted by $A \cup B$, is the set that contains those elements that are either in A or in B, or in both.

Let A and B be sets. The intersection of the sets A and B, denoted by A $\cap$ B, is the set containing those elements in both A and B.

Two sets are called disjoint if their intersection is the empty set.

Let A and B be sets. The difference (complement) of A and B, denoted by $A - B$, is the set containing those elements that are in A but not in B.

The complement of the set A, denoted by $\overline{\text{A}}$, is the complement of A with respect to Ω . Therefore, the complement of the set A is Ω - A.

2.3 Set Identities

1. Identity Laws

$$A \cap \Omega = A$$
$$A \cup \emptyset = A$$

2. Domination Laws

$$A \cup \Omega = \Omega$$
$$A \cap \emptyset = \emptyset$$

3. Idempotent Laws

$$A \cup A = A$$
$$A \cap A = A$$

4. Complementation Laws

$$\overline{(\overline{\mathrm{A}})} = A$$

5. Commutative Laws

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

6. Associative Laws

$$A \cup (B \cup C) = (A \cup B) \cup C$$
$$A \cap (B \cap C) = (A \cap B) \cap C$$

7. Distributive Laws

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

8. De Morgan's Laws

$$\overline{\mathrm{A} \cup \mathrm{B}} = \overline{\mathrm{A}} \cap \overline{\mathrm{B}}$$
$$\overline{\mathrm{A} \cap \mathrm{B}} = \overline{\mathrm{A}} \cup \overline{\mathrm{B}}$$

9. Absorption Laws

$$A \cup (A \cap B) = A$$
$$A \cap (A \cup B) = A$$

10. Complement Laws

$$A \cup \overline{\mathrm{A}} = \Omega$$
$$A \cap \overline{\mathrm{A}} = \emptyset$$

2.4 Functions

Given A function f from A to B

1. One To One: For a function to be one to one or every element $b \in B$ there is an element $a \in A$ with $f(a) = b$.
2. Onto: For a function to be onto $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain of f.

Definitions:

1. Function - Let A and B be nonempty sets. A function f from A to B is an assignment of exactly one element of B to each element of A. We write $f(a) = b$ if b is the unique element of B assigned by the function f to the element a of A. If f is a function from A to B, we write f : $A \to B$.
2. Domain - The set of possible values of the variables of a function.
3. Range - The set of all output values of a function.
4. Surjective - Another way to say onto.
5. Injective - Another way to say one to one.
6. One-to-one Correspondence (Bijection) - Both onto and one to one.

2.5 Sequences and Summations

2.6 Matrices

3 Induction and Recursion

3.1 Mathematical Induction

1. Principle of Mathematical Induction To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps, the base step and inductive step.
2. Base Step We verify that P (1) is true.
3. Inductive Step We show that the conditional statement $P(k) \to P(k+1)$ is true for all positive integers k.

Template for Proofs by Mathematical Induction

1. Express the statement that is to be proved in the form ?for all n ? b, P (n)? for a fixed integer b.
2. Write out the words ?BasisStep.? Then show that $P(b)$ is true, taking care that the correct value of b is used. This completes the first part of the proof.
3. Write out the words ?Inductive Step.?
4. State, and clearly identify, the inductive hypothesis, in the form ?assume that $P(k)$ is true for an arbitrary fixed integer $k \geq b$.?
5. State what needs to be proved under the assumption that the inductive hypothesis is true. That is, write out what $P(k+1)$ says.
6. Prove the statement $P(k+1)$ making use the assumption $P(k)$. Be sure that your proof is valid for all integers k with $k \leq b$, taking care that the proof works for small values of k, including $k = b$.
7. Clearly identify the conclusion of the inductive step, such as by saying ?this completes the inductive step.?
8. After completing the basis step and the inductive step, state the conclusion, namely that by mathematical induction, $P(n)$ is true for all integers n with $n \geq b$.

3.2 Strong Induction

1. <u>Strong Induction</u> To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps, the base step and inductive step.
2. <u>Base Step</u> We verify that P (1) is true.
3. <u>Inductive Step</u> We show that the conditional statement $[P(1) \wedge P(2) \wedge ... \wedge P(k)] \rightarrow P(k+1)$ is true for all positive integers k.

3.3 Recursive Algorithms

1. <u>Recursive</u> if it solves a problem by reducing it to an instance of the same problem with smaller input.

4 Counting

4.1 The Pigeonhole Principle

1. <u>The Pigeonhole Principle</u> -If k is a positive integer and k + 1 or more objects are placed into k boxes, then there is at least one box containing two or more of the objects.

4.2 Generalized Permutations and Combinations

1. Permutation Without Repetition - $P(n, r) = \frac{n!}{(n-r)!}$
2. Combination Without Repetition - $\binom{n}{k} = \frac{n!}{(n-k)! \times k!}$
3. Permutation With Repetition - $P(n, r) = n^r$
4. Combination With Repetition - $\binom{n}{k} = \frac{(n-r+1)!}{r!(n+1)!}$

5 Relation

5.1 Relations

1. Binary Relation from A to B is a subset of A × B.
2. Relation on a set A is a relation from A to A.
3. Reflexive if $(a, a) \in R$ for every element $a \in A$.
4. Symmetric if $(b, a) \in R$ whenever $(a, b) \in R$, for all $a, b \in A$
5. Antisymmetric A relation R on a set A such that for all $a, b \in A$, if $(a, b) \in R$ and $(b, a) \in R$, then $a = b$
6. Transitive if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$, for all $a, b, c \in A$.
7. equivalence relation For a relation to be equivalent it must be reflexive, symmetric, and transitive.
8. Partial Order If it is reflexive, antisymmetric, and transitive