Exam preparation cheetzheet:
Stuff from

MNF130V2020

May 19, 2020

1 Chapter 1

Propositional logic:. Logical $\wedge, \vee, \oplus$ are trivial.
Conditional statements (implication): $p \rightarrow q$, if p then $q \equiv p$ only if $q \equiv p$ is a sufficient condition for q.
In other words, q is a necessary condition for p. $p \rightarrow q$ is false then p is true and q is false and otherwise true. $\neg(p \rightarrow q) \equiv p \wedge (\neg q)$, $p \rightarrow q$ is equivalent to its contrapositive $\neg q \rightarrow \neg p$, but **not** to its **converse** $q \rightarrow p$ **or** its inverse $\neg p \rightarrow \neg q$.
Biconditional statements: $p \leftrightarrow q$ or expanded to $(p \rightarrow q) \wedge (q \rightarrow p)$.
De Morgan: $\neg(p \vee q) \equiv (\neg p) \wedge (\neg q)$; $\neg(p \wedge q) \equiv (\neg p) \vee (\neg q)$ Propositional logic can be represented by gates, creating combinational circuits which can represent **any** logical expression.
Quantifiers:

$\forall x(P(x) \rightarrow Q(x)) \equiv$ *for all x, if P(x) then Q(x)*
$\exists x(P(x) \wedge Q(x)) \equiv$ *there exists an x such that P(x) and Q(x)*

P(x),Q(x) are propositional functions and there is always a **domain** or **universe of discourse**, either implicit or explicitly stated,over which the variable ranges.
Negations of quantified propositions: $\neg \forall x P(x) \equiv \exists x \neg P(x); \neg \exists P(x) \equiv \forall x \neg P(x)$.

Theorem: A proposition that can be proved; **lemma:** a simple theorem, commonly used as part of a greater picture to prove other theorems; **proof:** A demonstration that a proposition is true, **collorary:** A proposition that can be proved as a consequence of a theorem that has just been proved. A collorary can be seen as “Side effects“ of the prooved theorem.
A **valid** argument is an argument using correct rules of inference based on tautologies (something that will always give the **true** conclusion in **any** given scenario. I. E. a tautology is something that is always true for all possible combinations.)
An **invalid** argument can be referred to as a **fallacy**, such as affirming the conclusion, denying the hypothesis, begging the question or circular reasoning. They can lead to false conclusions.
Some rules of inference:

- $[p \wedge (p \rightarrow q)]$ Modus Ponens
- $[\neg q \wedge (p \rightarrow q)]$ Modus Tollens
- $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$ Hypothetical syllogism (Transitivity)
- $[(p \vee q) \wedge (\neg p)] \rightarrow q$ Disjunctive syllogism
- $\{P(a) \wedge \forall x[P(x) \rightarrow Q(x)]\} \rightarrow Q(a)$ Universal modus ponens
- $\{\neg Q(a) \wedge \forall x[P(x) \rightarrow Q(x)]\} \rightarrow \neg P(a)$ Universal modus tollens
- $(\forall x P(x)) \rightarrow P(c)$ Universal instantiation
- $(P(c) arbitrary\ c) \rightarrow \forall x P(x)$ Universal generalization
- $(\exists x P(x)) \rightarrow (P(c)\ for\ some\ c)$ Existential instantiation
- $(P(c)\ for\ some\ element\ c) \rightarrow \exists x P(x)$ Existential generalization.

a Proofs

Trivial proof: A proof that $p \to q$ just shows that q is true witout using the hypothesis p.
Vacuous proof: A proof of $p \to q$ that just shows that the hypothesis p is false.
Direct proof: A proof of $p \to q$ that shows that the assumption of the hypothesis p implies the conclusion of q.
Proof by contraposition: A proof of $p \to q$ that shows that the assumption of the negation of the conclusion q implies the negation of the hypothesis p (in other words, proof of contrapositive).
Proof by contradiction: A proof of p that shows that the assumption of the negation of p leads to a contradiction.
Proof by cases: A proof of $(p_1 \vee p_2 \vee p_3 ... p_n) \to q$ that shows that each conditional statement $p_i \to q$ is true.
Statements of the form $p \leftrightarrow q$ require that both $p \to q$ and $q \to p$ be proved. It is sometimes necessary to give the two separate proof (usually a direct proof or a proof by contraposition); other times a string of equivalences can be constructed starting with p and ending with $q : p \leftrightarrow p_1 \leftrightarrow p_2 ... \leftrightarrow p_n \leftrightarrow q$.
To give a **constructive proof** of $\exists x P(x)$ is to show how to find an element x that makes $P(x)$ true. **Non-constructive existence proofs** are also possible, often using **proof by contradiction**.
One can **disprove** a universally quantified proposition $\forall x P(x)$ simply by giving a **counter example**, i.e. an object x such that $P(x)$ is **false**. One can, however, not proove it with such an example.
Fermat's last theorem: There are no positive integer solutions of $x^n + y^n = z^n \; if \; n > 2$.

An integer is **even** if it can be written as $2k$ for some integer k; an integer is **odd** if it can be written as $2k+1$ for some integer k. Every number is even or odd but not both. A number is **rational**, if it can be written as p/q with p being an integer and q strictly a non-zero integer.

2 Chapter 2

a Sets

Empty set: A set with no elements, commonly denoted as $\emptyset$. Do not confuse this with the set only containing the empty set. The difference is that the empty itself is empty, whereas the set containing the empty set has a single element.
Subset: $A \subseteq B \equiv \forall x(x \in A \to x \in B)$, whereas a proper subset is $A \subset B \equiv (A \subseteq B) \wedge (A \neq B)$, in other words, B has at least one element different from the set A.
Equality of sets: $A = B \equiv (A \subseteq B \wedge B \subseteq A) \equiv \forall x(x \in A \leftrightarrow x \in B)$.
Power set: $\mathcal{P}(A) = \{B|B \subseteq A\}$, the set of all subsets of A. A set with n elements has 2^n subsets.
Cardinality: $|S|$, the number of elements in S.
Some specific sets in regards to cardinality: $\mathbb{R}$ is the set of real numbers, represented by either finite or infinite decimals;
$\mathbb{N}$ is the set of all natural numbers (eg. $\{0,1,2,3,4,5...\}$), $\mathbb{Z}$ is the set of integers $\{...-2,-1,0,1,2,...\}$ and can also be denoted with only the positive or negative subset. $\mathbb{Q}$ is the set of rational numbers, where $\{p/q|p,q \in \mathbb{Z} \wedge q \neq 0\}$, $\mathbb{Q}^+$ is the set of positive rational numbers and a subset of $\mathbb{Q}$.
Set operations: $A \times B = \{(a,b)|a \in A \wedge b \in B\}$ (**Cartesian Product**); $\overline{A}$ is the set of elements in the universe which are **not** in A (**complement**); $A \cap B = \{x|x \in A \wedge x \in B\}$ (**intersection**); $A \cup B = \{x|x \in A \vee x \in B\}$ (**union**); $A - B = A \cap \overline{B}$ (**difference**); $A \oplus B = (A-B) \cup (B-A)$, (**symmetric difference/xor**)
Inclusion-exclusion (simple case): $|A \cup B| = |A| + |B| - |A \cap B|$
De Morgan's laws for sets: $\overline{A \cap B} = \overline{A} \cup \overline{B}$; $\overline{A \cup B} = \overline{A} \cap \overline{B}$
A **function** f from A (**the domain**) to B (**the co-domain**) is an assignment of a unique element of B to each element of A. Write $f : A \to B$. Write $f(a) = b$ if b is assigned to a. **Range** of f is $\{f(a)|a \in A\}$; f is **onto/surjective** $\equiv$ range (f) = B; f is **one-to-one/injective** $\equiv \forall a_1 \forall a_2 [f(a_1) = f(a_2) \to a_1 = a_2]$
If f is one-to-one **and** onto, it is **bijective** and the **inverse** function $f^{-1} : B \to A$ is defined by $f^{-1}(y) = x \equiv f(x) = y$.
If $f : B \to C$ and $g : A \to B$, then the **composition** $f \circ g$ is the function from A to C defined by $f \circ g(x) = f(g(x))$.
Rounding functions: $\lfloor x \rfloor$ is the largest integer less than or equal to x **floor function**; $\lceil x \rceil$ is the smallest integer greater than or equal to x **the ceiling function**.
Summation notation:

$$\sum_{n=1}^{n} a_i = a_1 + a_2 + a_3 + ... + a_n$$

Sum of first n positive integers:

$$\sum_{j=1}^{n} j = 1 + 2 + ... + n = \frac{n(n+1)}{2}$$

Sum of squares of first n positive integers:

$$\sum_{j=1}^{n} j^2 = 1^2 + 2^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Sum of geometric progression: (I don't think we did this in the course)

Two sets are said to have the **same cardinality** if there is a **bijection** between them. We can say that $|A| \leq |B|$ if there is a one-to-one function from A to B.
A set is *countable* if it is finite or there is a **bijection** from the positive integers to the set. **In other words**, if the elements of the set can be listed (e.g. $a_1, a_2, ...$). Sets of the latter type are called $countablyinfinite$ and the **cardinality of these sets are denoted with** $\aleph_0$. The empty set, the integers and the rational numbers **are countable**. The union of a countable number of countable sets is countable.
Schroder-Bernstein theorem: If $|A| \leq |B|$ and $|B| \leq |A|$ then it must be that $|A| = |B|$. This can be explained as if there is a one-to-one function from A to B and a one-to-one function from B to A, then there is a one-to-one and onto function from A to B.
Matrix Multiplication: The $(i, j)^{th}$ entry of **AB** is $\sum_{t=1}^{k} a_{it}b_{tj}$ for $1 \leq i \leq m$ and $1 \leq j \leq n$, where **A** is an $m \times k$ matrix and **B** is a $k \times n$ matrix.
Identity matrix I_n with 1's on the main diagonal and 0's elsewhere is the multiplicative identity.
Cardinality arguments can be used to show that some functions are **uncomputable**.
Matrix addition (+), Boolean meet ($\wedge$) and join ($\vee$) are done entry-wise; Boolean matrix product ($\odot$) is like matrix multiplication using boolean operators.
Transpose: $\mathbf{A}^t$ is the matrix whose $(i, j)^{th}$ entry is a_{ij} (the $(j, i)^{th}$ entry of **A**);
A is **symmetric** if $A^t = A$;