CMPE 16 final Study Guide

Final Exam : March 21st / Bring ID / Come Early!

Propositional Calculus (Logic)

Propositions are statements that are either True (1) or false (0)

Compound Propositions

$p \wedge Q$	P and Q	$P \cdot Q$	conjunction
$p \vee q$	P or q	$P + q$	disjunction
$\neg p$	Not p	$\bar{p}$, $!p$	negation
$p \rightarrow q$	p implies q	$\neg p + q$	implication
$p \leftrightarrow q$	p iff q		biconditional

Implications can be extrapolated from

- if p then q
- p implies q
- if p , q

Reverse:

- q if p
- q whenever p
- q is necessary for p

Contrapositive : If $p \rightarrow q$, $\neg q \rightarrow \neg p$ is always valid

Operator Precedence

$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

where 1 binds the closest (think PEMDOS)

Logic (cont.)

Identity Laws	$p \wedge T = p$	$p \vee F = p$
Domin. Laws	$p \vee T = T$	$p \wedge F = F$
Idemp. Laws	$p \vee p = p$	$p \wedge p = p$
Double Neg. Law	$\neg(\neg p) = p$	
Comm. Laws	$p \vee q = q \vee p$	$p \wedge q = q \wedge p$
Assoc. Laws	$(p \vee q) \vee r = p \vee (q \vee r)$	$(p \wedge q) \wedge r = q \wedge (p \wedge r)$
Distr. Laws	$p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$	$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r$

* Given on Final

Boolean Algebra

A	B	AND	OR	XOR	NEG(A)
0	0	0	0	0	1
0	1	0	1	1	1
1	0	0	1	1	0
1	1	1	1	0	0

DeMorgan's Law

$$\neg(p \vee q) = \neg p \wedge \neg q$$
$$\neg(p \wedge q) = \neg p \vee \neg q$$

Principal of Duality

if you flip the 0s and 1s, flip the $\vee$s and $\wedge$s
and the validity of any theorem is preserved

Absorption Law

p	q	p ∧ q	p ∨ (p ∧ q)
0	0	0	0
0	1	0	0
1	0	0	1
1	1	1	1

Proof of Absorption Law

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

$p \vee (p \wedge q)$	Identity
$(p \wedge T) \vee (p \wedge q)$	Distributive
$p \wedge (T \vee q)$	Domination
$p \wedge T$	Identity
p	

Tautology - a statement that is always true
can be proven using tables

p	q	p∨q	¬p	¬p∧(p∨q)	[¬p∧(p∨q)] → q
0	0	0	1	0	1
0	1	1	1	1	1
1	0	1	0	0	1
1	1	1	0	0	1

should be all 1s if you did it right

Disjunctive Normal form (Sum of Products)

Take all the rows that are 1, and them together, or the terms
Force all the propositions to 1 with negation

Conjunctive Normal form (Product of Sums)

Take all the 0 rows, or them together, AND the terms
Force everything to 0 with negation

p	q	r	Out
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

$(\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (p \wedge q \wedge \neg r)$ DNF

$(p \vee q \vee r) \wedge (p \vee q \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (\neg p \vee \neg q \vee \neg r)$ CNF

Sets

U	universe of discourse
$\{,\}$	set
$\in$	element of
$\notin$	not an element of
$\subseteq$ / $\subset$	subset / proper subset

Multiple items of the same kind does not change a set

$A = \{1, 2, 3\}$, $B = \{1, 1, 2, 3\}$, $A = B$

Special sets

natural numbers	$\{0, 1, 2, 3...\}$
Integers	$\{...-1, 0, 1...\}$
Real Numbers / Rational Numbers	$\{p/q : p \in \mathbb{Z}, q \in \mathbb{Z}^+\}$ ← denotes positive integers
	$\mathbb{R} - \mathbb{Q}$

$\emptyset = \{\}$ is the empty set
* $\emptyset \notin \emptyset$

When denoting sets, ∞ can never be in ([ ]) square brackets.

Set Cardinality is the number of distinct elements of a set.
Denoted by $|s|$

$|\emptyset| = 0$ $\emptyset$ contains no elements
$|\{\emptyset\}| = 1$ $\emptyset$ is an element

Countable Sets

$\mathbb{N}$ is a countable set
Therefore if a set can be indexed by $\mathbb{N}$, it to is countable

Ordered Pairs

denoted (x, y)
Cartesian Product of (X, Y) is denoted $(X \times Y)$
Set of all well-ordered pairs $x \in X$, $y \in Y$
Tuples are the same as pairs but of n sets

Power Sets

denoted by $P(S)$
$|P(s)| = |2^S| = 2^{|S|}$

$S = \{0, 1, 2\}$
$|P(s)| = 2^{|S|} = 8$

1	$\emptyset$
2	0
3	1
4	2
5	{0, 1}
6	{0, 2}
7	{1, 2}
8	{0, 1, 2}

$\cup$ Union

Intersection

$-$ Difference (things in A, not in B)

^{c} Compliment | (thing in A, not in B and visa versa)

$\oplus$ Symmetric Difference (XOR)

$A = \{0, 1, 2\}$ $B = \{0, 1, 3\}$

$A \cup B = \{0, 1, 2, 3\}$ $A^c = \{3\}$

$A - B = \{2\}$

$A \overset{\text{int.}}{} B = \{0, 1\}$

$A \oplus B = \{2, 3\}$

All propositional identities apply to sets where

$\wedge \rightarrow \cap$

$\vee \rightarrow \cup$

$\neg \rightarrow {}^c$

Show the $(A \cup B)^c = A^c \wedge B^c$ *DeMorgan's Law

$$
\begin{aligned}
(A \cup B)^c &= \{x \mid \neg(x \in A \vee x \in B)\} \\
&= \{x \mid \neg(x \in A) \wedge \neg(x \in B)\} \\
&= \{x \mid x \in A^c \wedge x \in B^c\} \\
&= A^c \wedge B^c
\end{aligned}
$$

Russells Paradox

Does the set of all sets that does not contain itself, contain itself?

Predicates and Quantifiers

Predicates $P(x)$ takes input x and returns T or F
Predicates that take an n-tuple are n-ary predicates
Predicates return truth sets in respect to Univ. of discourse

$\forall_x P(x)$ For all x $P(x)$
$\exists_x P(x)$ there exists an x $P(x)$

It is impossible to find the truth value of an unbounded variab

$\neg \forall_x P(x) = \neg (P(x_1) \wedge P(x_2) \wedge P(x_n))$ * By DeMorgan's
$\exists_x \neg P(x) = \neg P(x_1) \vee \neg P(x_2) \vee P(x_n) =$ [illegible]

$\neg \exists_x P(x) = \forall_x \neg P(x)$
$\exists! x P(x)$ one and only one x

Variable cannot be rebound.
i.e. $\forall_x (\forall_x (P(x))$

Proofs

Hypothesis : $H_1, H_2, \cdots, H_n$
Conclusion : C
Proof $H_1 \wedge H_2 \cdots H_n \rightarrow C$ is shown to be a tautology

Hypothesis is a sequence of propositions
Reach the Conclusion through rules of inference

Rules of Inference

Modus Ponens

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

Modus Tollens

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

Hypothetical Syllogism

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

Disjunctive Syllogism

$$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$$

Addition

$$\begin{array}{l} p \\ \hline \therefore p \vee q \end{array}$$

Simplification

$$\begin{array}{l} p \wedge q \\ \hline \therefore q \end{array}$$

Resolution

$$\begin{array}{l} \neg p \vee r \\ p \vee q \\ \hline \therefore q \vee r \end{array}$$

acuous Proof – don't need a hypothesis

nvial Proof – Everything is in the conclusion

of by Contraposition

$P \rightarrow q \iff \neg q \rightarrow \neg p$

ove that $\sqrt{2}$ is irrational ← THIS IS LIKELY ON THE FINAL

y contradiction:

$\sqrt{2}$ is rational so $\exists a, b \in \mathbb{Z}$, $b \neq 0$, $\gcd(a, b) = 1$

$\sqrt{2} = a/b$

$2 = a^2/b^2$

$a^2 = 2b^2$ (a^2 even, so a even, so $\exists c \in \mathbb{Z}$, $a = 2c$)

$2 = a^2/b^2$

$2b^2 = 4c^2$ so $b^2 = 2c^2$, so b^2 is even, so b is even

evenly divides a and b

$\gcd(a, b) \neq 1$

Contradiction

Proof by cases

each implication $p_i \to q$ in $(p_1 \vee p_2 \vee \dots \vee p_n) \to q$ must be proven

$(p_1 \vee p_2 \vee \dots p_n) \to q \leftrightarrow [(p_1 \to q) \wedge (p_2 \to q) \wedge \dots \wedge (p_n \to q)]$

Existance Proof

if asked to find $\exists x P(x)$, find that x

Counterexample

Prove $\neg \forall_x P(x)$ OR $\exists_x \neg P(x)$

Provide counterexample x

Functions

denoted by:

- f maps A onto B
- $f : A \to B$
- $f \subseteq A \times B$
- $(a, b) \in f$

set of ordered pairs

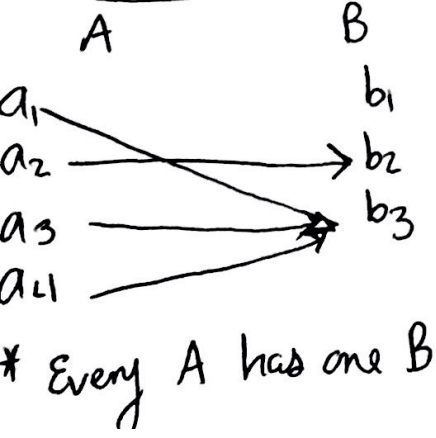
In order for something to be a function, each A must map to a unique B

$\forall a \in A \; \exists! \; b \in B (f(a) = b)$

$f(a) = b$

- b is the image of a
- a is the pre-image of b

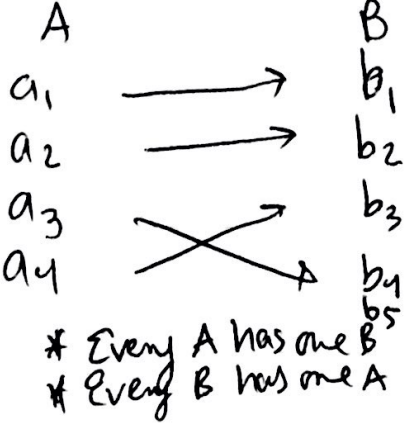
FUNCTION



* Every A has one B

INJECTIVE/

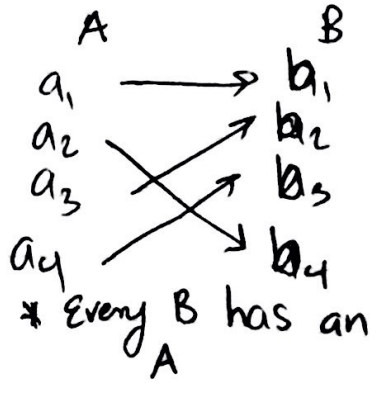
ONE-TO-ONE



* Every A has one B
* Every B has one A

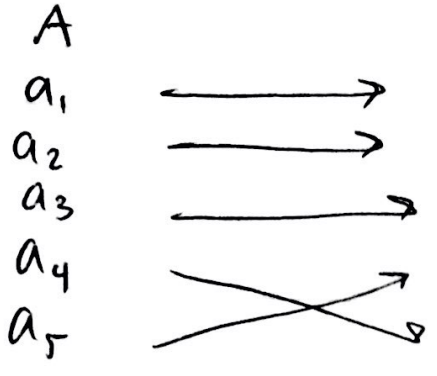
SURJECTIVE/

ONTO



* Every B has an A

One-to-One Correspondense



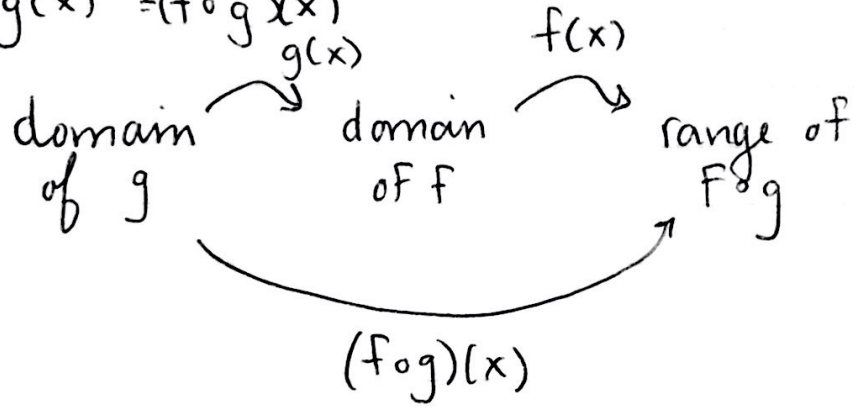
Correspondenses

- One to one ~~functions~~ are when functions are ~~1~~ onto AND one-to-one
- f becomes invertible

$f(a) = b \rightarrow f^{-1}(b) = a$

Composition of Functions

$f(g(x)) = (f \circ g)(x)$



$f(x) + g(x) = (f+g)(x)$

$f(x) \cdot g(x) = (f \cdot g)(x)$

Infinite sets become countable iff you can create a one-to-one correspondense with the natural numbers (which we know to be countably infinite)

$|\mathbb{Z}| = |\mathbb{N}|$

0	1	-1	2	-2	3	-3	...
↕	↕	↕	↕	↕	↕	↕	...
1	2	3	4	5	6	7	

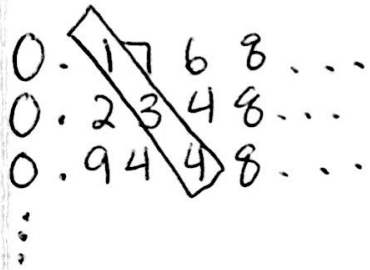
$\mathbb{Z}$ can be mapped to $\mathbb{N}$ so it is countable. $|\mathbb{Z}| = |\mathbb{N}|$ because

Diagonalization

tinyurl.com/diagonalization
↑ The most painless way of understanding this

Proof by contradiction

Assume there are an infinite amount of numbers between 0 and 1



∴ According to our hypothesis, there should be no number (0, 1) not in our set.

By changing one digit (in the box) diagonally, you generate a new number (0, 1) that is unique. This is a contradiction showing that some infinities are different sizes.

Floor & Ceiling

(⌊ ⌋) floor - round down to nearest int
(⌈ ⌉) ceiling - round up to nearest int

Triangle Inequality

$(\forall x \in R)(\forall y \in R)(|x+y| \leq |x| + |y|)$

Proven by cases

1.	$x < 0$	&&	$y < 0$
2.	$x \geq 0$	&&	$y \geq 0$
3.	$y < 0$	&&	$x \geq 0$
4.	$y \geq 0$	&&	$x < 0$

Sequences

$\{a_i\}_m^n$
function maps $\mathbb{N}$ where $m \leq i \leq n$

Summations

$$\sum_{i=m}^{k} a_i = a_m + a_{m+1} + \ldots + a_k$$

```
for (i = m; i ≤ k; i++){
    sum += a_i;
}
```

Summations can be broken ~~into m~~ by removing the first or last element

$$\sum_{i=0}^{k} a_i = a_0 + \sum_{i=1}^{k} a_i$$

Closed forms

$$\sum_{k=1}^{n} (2k-1) = 2\sum_{k=1}^{n} k - \sum_{k=1}^{n} 1$$

$$\frac{2(n+1)n}{2} - n$$

$$n^2 + n - n$$

$$n^2$$

$$\sum_{k=1}^{n} 2k-1 = \boxed{n^2}$$

Factors

Positive integers are prime iff they have two positive factors (1 and itself)

2 is a prime number

Composite integers have more than two factors

Fundamental Theorem of Arithmetic

if n is a positive integer, there are a finite list of primes and non-negative integers such that

$$n = p_1^{i_1} \cdot p_2^{i_2} \cdot p_3^{i_3} \cdots p_m^{i_m}$$

i.e. $6 = 2^1 \cdot 3^1$

$9 = 2^0 \cdot 3^2$

$42 = 2^1 \cdot 3^1 \cdot 7^1$

Division

$a = d \cdot \lfloor \frac{a}{d} \rfloor + a \bmod d$

$a = d * \text{int}(a/d) + (a \,\%\, d)$

a = dividend
d = divisor
q = quotient
r = remainder

Modular Arithmetic

$a \bmod m$ remainder of $\frac{a}{m}$

if $a, b \in \mathbb{Z}$ AND $m \in \mathbb{Z}^+$ AND $a \bmod m = b$

$a \equiv b \pmod m$

a is congruent to $b \pmod m$

LCM

smallest integer divisible by both

$\text{lcm}(m,n) = \min\{k > 0 : m \mid k \wedge n \mid k\}$

GCD

largest integer that divides both m and n

$\gcd(m,n) = \gcd(n \bmod m, m)$

$= \max\{k : k \mid m \wedge k \mid n\}$

There are an infinite number of primes

Proof by Contradiction

Assume there are a finite number of primes

$\{P_1, P_2, P_3 \ldots P_n\}$ = Primes

Q is the product of all Primes

$Q + 1$ is not divisible by any prime $\in$ Primes

Q is either a prime or is divisible by a prime not in Primes