CSE 321 Review Session

Dave Bacon

Final

1 hour, 50 minutes.

Closed book. (You can bring a calculator.) $\binom{52}{2}$ ok. $\frac{52 \cdot 51}{2} = 26 \cdot 51$

11 Problems.

~3 problems from before midterm material. Rest from after midterm.

Basic Logic

Basic boolean logic

$p \wedge q$ $p \to q$ $\neg p$, etc, etc. $p \vee q$

Conditional, converse, contrapositive, inverse

$p \to q$, $q \to p$, $\neg q \to \neg p$, $\neg p \to \neg q$

Tautology, contradiction, contingency

T F either T or F.

You will be given a list of logical equivalences

Example problem: Show that $(p \wedge q) \to (p \vee q)$ is a tautology

1. $\neg(p \wedge q) \vee (p \vee q)$ (alt. def of $a \to b \equiv \neg a \vee b$
2. $(\neg p \vee \neg q) \vee (p \vee q)$ Demorgans law
3. $(\neg p \vee p) \vee (q \vee \neg q)$ Commutivity & Associativity of $\vee$
4. $T \vee T$ ($a \vee \neg a \equiv T$ negation law)
5. T

Predicates and Qualifiers

Universal quantifier, For all x has same domain P(x)

Predicates + Qualifiers

$\forall x\, Q(x)$ For all x, Q(x)

Existential quantifier, There exists

$\exists x\, Q(x)$

order matters $\forall x \forall y\, Q(x,y)$? $\exists x \exists y\, Q(x,y)$

$\forall x \exists y$ & $\exists x \forall y$ different.

Negating, [translating to sentences], nesting, showing equivalence

Example: Show $\forall x\,(P(x) \wedge Q(x))$ and $(\forall x\, P(x)) \wedge (\forall y\, Q(y))$ are equivalent

[This changes if its $\vee$]

Sps $\forall x\,(P(x) \wedge Q(x))$ is true.

For all a in domain $P(a) \wedge Q(a)$ is true

$P(a)$ is true and $Q(a)$ is true.

$\forall a P(a)$ is true simr $\forall a\, Q(a)$ is true. $\Rightarrow (\forall x P(x)) \wedge (\forall x\, Q(x))$

Similarly for inverse direction.

Rules of Inference, Proofs

We'll provide a list. Know how to use them to prove statements.

Rules of inference Proofs

Rules of Inference for nested qualifiers (Universal instantiation, etc.)

Proof methods, Direct proof, Proof by Contraposition, Proofs by Contradiction

$p \to q$

Assume p is true $\to \to \to$ q is true.

Contraposition

$\neg q \to \neg p$ Start with $\neg q$ is true q is false.

Contradiction

assume statement is false

$\Rightarrow$ contradiction. $q \wedge \neg q$.

Sets

Definition of set. Subsets. Empty set. What it means for two sets to be equal.

ϕ Show this ($A=B$) SETS.

$A \subseteq B \wedge B \subseteq A$

Power Set

Set of all subsets.... $\{ \{\}, \{A\}, ... \}$ $P(A)$ $|P(A)| = 2^{|A|}$

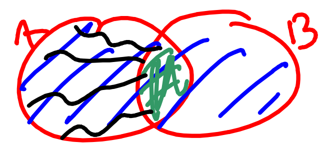
Cartesian product of sets

$A \times A = \{ (a,b) \mid a \in A \wedge b \in A \}$

$U - A = \bar{A}$

Union of sets, intersection of sets, difference of sets, complement of a set

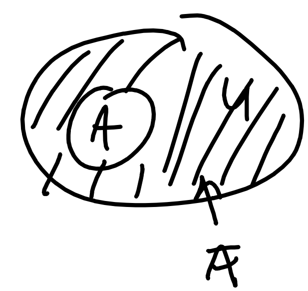
$A \cup B$, $A \cap B$



$A \cup B$

$A \cap B$

$\bar{A}$ in U



Set identities.

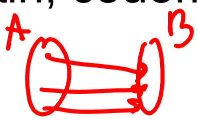
Example: Show that $\underbrace{\overline{A \cup (B \cap C)}}_{L} = \underbrace{(\bar{C} \cup \bar{B}) \cap \bar{A}}_{R}$

To show $x \in L \Rightarrow x \in R$

$x \in R \Rightarrow x \in L$.

Functions

Domain, codomain. Image, preimage. Range.

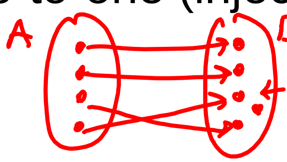


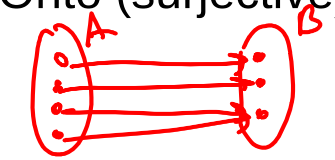
domain A codomain B

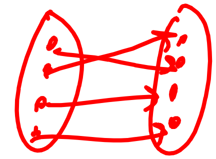
$a \to b$

Functions

One-to-one (injective). Onto (surjective). One-to-one correspondence (biject~~ion~~ ve)







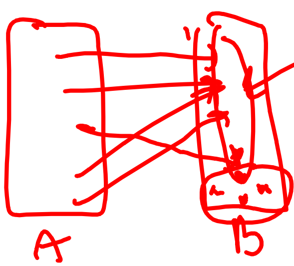
Composing functions. Inverse of a function.

$f \circ g$ $\quad g: A \to B$, $f: B \to C$ $\quad f \circ g : A \to C$.

f^{-1} doesn't always exist.

Example question: f:Z->Z such that f(x)=x^2. Is one-to-one? Is Onto?

No. $f(-1) = f(1)$ No. no $f(a) = -1$.



range.

not range.

b is the image of a.

$f(a) = b$.

Functions

Domain, codomain. Image, preimage. Range.

One-to-one (injective). Onto (surjective). One-to-one correspondence (bijection)

Composing functions. Inverse of a function.

Example question: $f:Z\text{->}Z$ such that $f(x)=x^2$. Is one-to-one? Is Onto?

Primes, and GCD

Prime, composite. Fundamental theorem of arithmetic.   Primes + GCD

Greatest common divisor. Least common multiple. Relatively prime.

gcd(a,b)   lcm(a,b)   no common factors, gcd(a,b)=1

Representing numbers in a base. Modular ~~arithametic.~~ stuff.

When does an inverse exist?

$(5 \cdot 10 \bmod 7 = 1)$

multiplicative inverses, does 5 have an mult inverse modulo 11?

$5x \equiv 1 \pmod{11}$? prime

additive inverse: $x + 5 \equiv 1 \pmod{11}$ always exist.

Modular exponentiation.

$a^k \bmod N$ $k = k_0 + 2k_1 + 4k_2 + \cdots + 2^{j-1}k_j$ $k_i \in \{0,1\}$

The Euclidean algorithm.

$a^{k_0} a^{k_1 \cdot 2} a^{k_2 \cdot 4} \cdots a^{k_j 2^{j-1}} \bmod N$

a, a^2, a^4, by repeated squaring

Know how to do it.

$\gcd(a,b) = g$

$sa + tb = g$, $s,t \in \mathbb{Z}$.

$1x \equiv 1 \pmod 4$ $x = 1$

$2x \equiv 1 \bmod 4$ no x?

Induction

Induction

Basic inductive proof: P(k) define.

Basis step: Verify P(1) is true.

Inductive hypothesis: $\boxed{\text{P(k)}}$

Inductie step: Show P(k)->P(k+1) is true (for all positive k)

give → $\boxed{}$

basis case P(1), P(2)

strong.

Strong induction. $P(k) \to P(k+1)$ $P(1), \dots, P(k-1), P(k) \to P(k+1)$

Structural induction. Recursively defined sets.

Basis: $3 \in A$

Recursive: If $a \in A$, then $3+a \in A$

$\{3, 6, 9, 12, \dots\}$

Example: (Prove $\sum_{i=1}^{n} 2^i = 2^{n+1} - 1$ for all non-negative n.)

$a \in A$

prove a div. by 3.

basis: $3 \in A$ (basis of def.) 3 is div by 3 ✓

recursive: $a \in A$ a div by 3.

$\Rightarrow$ a+3 div by 3 new element satisfy our property.

Basics of Counting

Counting.

- Sum rule, product rule.

if $A_1 \cap A_2 = \emptyset$

$|A_1 \cup A_2| = |A_1| + |A_2|$

$$\boxed{|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|}$$

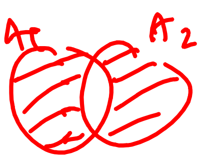
- How many bitstrings of length ten either begin with a ~~single~~ 0 or end with a ~~single~~ 1, but not both?

exclusive or (but not both.)

$A_1 = \{$bitstring start with a single 0$\}$ $\quad |A_1| = 2^9$

$A_2 = \{$bit string ends with a single 1$\}$ $\quad |A_2| = 2^9$

$|A_1 \cap A_2| = 2^8$



$$\underbrace{|A_1 \cup A_2 - A_1 \cap A_2|}_{\text{exclusive-or}} = |A_1| + |A_2| - 2|A_1 \cap A_2|$$

0 ... 1

$= 2^9 + 2^9 - 2 \cdot 2^8$

$= 2^9 = 512$

$2^{127} \bmod 2 = 0$

Pigeon Hole

$N=6 \quad K=14$

$\lceil \frac{6}{14} \rceil = 1$

$N=1$, $K=14$, $\lceil \frac{1}{14} \rceil = 1$

Pigeons, holes, function from pigeon to hole.

Pigeon hole principle

Standard pigeon hole principle, Generalized pigeon hole principle

Define your pigeons

Define your holes

Define function pigeons to holes.

Stand n pigeons and $n-1$ holes

f: pigeons $\to$ holes.

$\exists$ hole that has 2 pigeons.

deg $= 0$ and deg $= n-1$ at same not possible

$V \xrightarrow{F} S$ $|S| = n-1$

$|V| = n$

Example: Graph G with n vertices.

Prove $\exists$ two vertices of the same degree.

assume all vertices have diff degree...

$d_1, \ldots, d_n$ $d_i \neq d_j$

$0 \leq d_i \leq n-1$

$0, 1, \ldots, n-1$

$\Rightarrow$ not possible deg 0 $\wedge$ deg $n-1$

N pigeons K holes at least $\lceil \frac{N}{K} \rceil$ pigeons in one hole

$\lceil \frac{6}{14} \rceil = 1$ $\lceil \frac{1}{14} \rceil = 1$

$\lceil x \rceil =$ smallest integer $\geq x$.

Permutations

Selecting ~~k~~ r objects in order from a set of size n. P(n,r)=n!/(n-r)!   Permutations

$P(n,r) = \frac{n!}{(n-r)!}$ without replacement:

$\underbrace{n}_{1}\ \underbrace{n-1}_{2}\ \underbrace{n-2}_{3} \cdots \underbrace{n-r}_{r}$ $P(n,r) = n(n-1)\cdots(n-r)$

Example: How many permutations of the letters ABCDEFGH contain ABC?

BACDEFHG is good   BAD is bad

Bad   is a perm   is not perm.

DEABCFGH is good   (ABC, D, E, F, G, H)   6

$P(6,6) = 6!/(6-6)! = 6!$

perm of length 5 containing ABC.

ABC * *   20   * ABC *   20   * * ABC   20

5 4

$20+20+20 = 60$

Combinations

Combinations

Selecting ~~k~~ r objects from a set of size n. C(n,r)=n!/[(n-r)!r!].

$$C(n,r) = \binom{n}{r} = \frac{n!}{(n-r)!\,r!} = \frac{P(n,r)}{r!}$$

Example: How many ways are there to select five players from a 10-member tennis team to make a trip to another school?

$r=5$ $\qquad$ $n=10$

$$\binom{10}{5} = \frac{10!}{5!\,5!}$$

Binomial Theorem

Know it! Binomial coefficients.

Binomial Theorem

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

$C(n,k)$

Combinatorial proof.

Example: Give comb. proof of $\sum_{i=0}^{n} \binom{n}{i} = 2^n$

Constructing power set of a set of cardinality n

$|A|=n$ $|P(A)|$

powerset $\Rightarrow$ include each a_i or not include a_i to make a subset

construct all subsets of size i $\binom{n}{i}$ $\sum_{i=0}^{n}\binom{n}{i}$

Probability

Uniform probability Pr(E)=|E|/|S|. Reduces to counting.

Probability

$Pr(E) = \frac{|E|}{|S|}$

$\boxed{Pr(\overline{E})=1-Pr(E)}$ trick to save your hand.

$$Pr(E_1 \cup E_2) = Pr(E_1) + Pr(E_2) - Pr(E_1 \cap E_2)$$

Example: What is the probability that a postitive integer selected at random from the set of postive integers not exceeding 100 is divisble by either 2 or 5?

$E_1 = \{ \text{div. by } 2 \}$ $|E_1| = 50$ $Pr(E_1) = \frac{1}{2} = \frac{50}{100}$

$E_2 = \{ \text{div by } 5 \}$ $|E_2| = 20$ $Pr(E_2) = \frac{1}{5} = \frac{20}{100}$

$|E_1 \cap E_2| = 10$ $Pr(E_1 \cup E_2) = \frac{1}{2} + \frac{1}{5} - \frac{1}{10} = \frac{3}{5}$

$Pr(E_1 \cap E_2) = \frac{1}{10}$

$|S| = 100$

Conditional Probability

$$\Pr(E|F) = \frac{\Pr(E \cap F)}{\Pr(F)}$$

Conditional Probability

Example: What is the conditional probability that a family with two children has two boys, given that they have at least one boy? Assume BB, BG, GB, GG are equally likely.

E

F

$$\Pr(F) = \frac{3}{4}$$

$$\Pr(E \cap F) = \frac{1}{4}$$

$$\Pr(E|F) = \frac{1/4}{3/4} = \frac{1}{3}.$$

More Probability

Independence

$$\Pr(E \cap F) = \Pr(E)\Pr(F)$$

Bernoulli trials

p H $\quad 1-p$ T

$$\Pr(\text{exactly } k \text{ H's in } n \text{ trials}) = \binom{n}{k} p^k (1-p)^{n-k}$$

Birthday paradox

$$\Pr(E) = 1 - \Pr(\overline{E})$$

Bayes Theorem

$$\Pr(F \mid E) = \frac{\Pr(E \mid F)\Pr(F)}{\Pr(E \mid F)\Pr(F) + \Pr(E \mid \overline{F})\Pr(\overline{F})} = \frac{\Pr(E \mid F)\Pr(F)}{\Pr(E)}$$

Random Variables, Expected Value

What is a random variable? Two views (function or induced distribution.)

$X: S \to \mathbb{R}$.   induced prob. distribution subset of $\mathbb{R}$.

Expected value of random variable. Variance. Linearity of expected value.
Independent random variables.

$$E[X] = \sum_{s \in S} \Pr(s)\, X(s) = \sum_k \Pr(X(s)=k)\, k.$$

all values take by the random variable.

$V[X] = E[X^2] - E[X]^2$

Example: A coin is flipped until it comes up tails. What is the expected number of flips until this coin comes up tails?

X

$\{T\}$ $X(\{T\}) = 1$ $\Pr(\{T\}) = \frac{1}{2}$

$\{HT\}$ $X(\{HT\}) = 2$ $\Pr(\{HT\}) = \frac{1}{4}$

$\{HHT\}$ $= \frac{1}{8}$

$\{HHHT\}$

$\vdots$

$E[X_1 + X_2] = E[X_1] + E[X_2]$

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

$$\sum_{i=1}^{n} a^i = a + a\left(\sum_{i=1}^{n} a^i\right) - a^{n+1}$$

$$S = \frac{a - a^{n+1}}{1-a}$$

$$E[X] = 1 \cdot \frac{1}{2} + 2 \cdot \frac{1}{4} + 3 \cdot \frac{1}{8} + \cdots = \sum_{i=1}^{\infty} i \left(\frac{1}{2}\right)^i = 2$$

Relations

Definition. Digraph form.

Relations.

$a \to b$

aRb

$(a,b) \in R$

Reflexive, symmetric, anti-symmetric, transitive

Equivalence relation, equivalence class.

Closures.

Example: Let R be a relation on integers, such that (x,y) in R iff x does not equal y.
Is R reflexive? Symmetric? Transitive?

$x \neq y$

No $(x,x) \notin R$

Yes

$xRy \wedge yRz \overset{?}{\Rightarrow} xRz$

$x=2 \quad y=3 \quad z=2$

$2R3 \quad 3R2 \quad 2R2$

$T \quad T \quad F$

Graphs

Basic definitions. Directed, undirected. Simple. Multigraph. Psuedograph. Degree of vertex. Handshaking theorem. Bipartite graphs. Connectivity. Graphs.

Paths. Simple paths. Euler paths. Circuits. Euler circuits. Hamilton paths. Hamilton circuits.

Constructive algorithm for Euler circuits/paths.

Example: Does the following graph have a Euler circuit? If so construct one.