Massachusetts Institute of Technology
6.042J/18.062J: Mathematics for Computer Science
Handout 54
May 24, 1996
Prof's Albert R. Meyer and Ronald L. Rivest

Final Exam

This is an OPEN BOOK Final: you may refer to books, handouts, or your own course notes. (Calculators are not allowed.) You may use in your problem solutions any of the mathematical results given in lectures, recitations, or the course text. There are twelve problems of roughly equal weight to complete within three hours.

Write all solutions in the exam book. You may use the back of the pages if you need more space.

Good luck!

Name: ______________________________

Problem	Grade
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
Total	

Problem 1. Let A be a set and R be a binary relation on A. For each of the statements in the box on the left below, indicate the number of the formula in the box on the right expressing that property. (Recall that the *composite* of two binary relations R and S, written $S \circ R$, is the relation $\{(a, c) \mid \text{there exists some } b \text{ such that } (a, b) \in R \text{ and } (b, c) \in S\}$. R^T is the *transpose* of R, i.e., $R^T = \{(a, b) \mid (b, a) \in R\}$, and I denotes the *identity* relation on A, i.e., $I = \{(a, a) \mid a \in A\}$.)

a.	R is transitive	
b.	R is antisymmetric	
c.	R is reflexive	
d.	R is symmetric	
e.	R is a bijection	
f.	R is an equivalence relation	
g.	R is a partial order	

1.	$R = R^T$
2.	$R \circ R \subseteq R$
3.	$R \cap R^T \subseteq I$
4.	$R \cap R^T \subseteq I \subseteq R \circ R \subseteq R$
5.	$I \subseteq R$
6.	$R \circ R^T = R^T \circ R = I$
7.	$I \subseteq R \circ R \subseteq R \subseteq R^T \cap R$

Problem 2. **(a)** Consider the set of polynomials with **integer** coefficients. We claim this set is countable. In fact, the proof is very similar to Problem 5 on Problem Set 4 (see Appendix). However, we need to choose a new definition of the norm. In particular, we wish to maintain the property that the number of polynomials that have norm k is finite for any k. Which of the following definitions of norm are appropriate? (There may be more than one correct answer; list them all.) We let d denote the degree of the polynomial and $a_0, a_1, a_2, \ldots, a_d$ denote the coefficients.

(i) $\max(d, a_0)$

(ii) $\max(d, a_0, a_1, a_2, \ldots, a_d)$

(iii) $\max(d, |a_0|, |a_1|, |a_2|, \ldots, |a_d|)$

(iv) $\max(|a_0|, |a_1|, |a_2|, \ldots, |a_d|)$

(v) $\max(d, a_0^2, a_1^2, a_2^2, \ldots, a_d^2)$

Answer: ____________________

(b) A real number is called *algebraic* if and only if it is the root of a non-zero polynomial with integer coefficients. You may recall that every nonzero polynomial has a finite number (possibly zero) of real roots. Are the algebraic numbers countable or uncountable?

Answer: ____________________

(c) Some numbers (such as π or e) cannot be expressed as a root of a polynomial with integer coefficients. These numbers are called the transcendental numbers. Is the set of transcendental numbers countable or uncountable?

Answer: ____________________

Problem 3. In this problem, A, B and C denote arbitrary sets. f and g are functions as specified in each part and I denotes the identity function. For each statement indicate whether it is **T**rue or **F**alse. No explanation is required.

T F There exists an injection (one-to-one) $f : A \to B$ if and only if there exists a surjection (onto) $g : B \to A$.

T F Let $f : A \to B$ and $g : B \to A$. $f \circ g = I$ implies $g \circ f = I$.

T F Let $f : A \to B$ and $g : B \to C$. If both f and g are injections, then $g \circ f$ is an injection.

T F Let $f : A \to B$ and $g : B \to C$. $g \circ f$ is a surjection implies both f and g are surjections.

T F Let $f : A \to B$ be an injection. If $|B| \leq |A|$, then f is a bijection.

Problem 4. Answer **T** or **F**:

T F The mapping $f_a : Z_p \to Z_p$ defined by

$$f_a(x) = ax(\text{mod } p)$$

is a bijection for any nonzero $a \in Z_p$, when p is prime.

T F For all a, b in $\mathbb{N}$, $\gcd(a^2b, ab^2) = ab$.

T F If $a^{-1}(\text{mod } b)$ exists, then so does $b^{-1}(\text{mod } a)$.

T F Let $\lambda(n)$ denote the number of distinct prime factors of n. Then $\lambda(n) = \Omega(\lg \lg n)$.

Problem 5. Answer **T** or **F**:

T F Adding k edges to an undirected graph increases its chromatic number (the number of colors needed to color the vertices) by at most k.

T F The number of shortest paths in an n-vertex undirected graph is $O(n^2)$. (Note: there may be more than one shortest path between two vertices.)

T F Reversing the directions of all edges in a directed graph leaves the number of simple directed cycles unchanged.

T F If an undirected graph has the degree of every vertex divisible by a prime p, then p must evenly divide the number of edges.

Problem 6. Given events $A_1, \cdots, A_n$, let N be the random variable equal to total number of these events which occur in a single trial. Let B be the event that none of the A_i occurs. When the events are *independent*, we can prove that the likelihood of B decreases exponentially with the expected value of N, namely

$$\Pr(B) \leq e^{-E(N)}.$$

Here is a proof—with justifications for many of the lines omitted.

Proof.

$$\begin{aligned}
B &= \overline{A_1} \cap \cdots \cap \overline{A_n} && \text{by } (a)____________. \text{ Hence,} \\
\Pr(B) &= \Pr(\overline{A_1} \cap \cdots \cap \overline{A_n}) && \\
&= \prod_{i=1}^{n} \Pr(\overline{A_i}) && \text{by } (b)____________ \\
&= \prod_{i=1}^{n} (1 - \Pr(A_i)) && \text{by } (c)____________ \\
&\leq \prod_{i=1}^{n} e^{-\Pr(A_i)} && \text{by } (d)____________ \\
&= e^{-\sum_{i=1}^{n} \Pr(A_i)} && \text{by } (e)____________ \\
&= e^{-E(N)} && \text{by } (f)____________.
\end{aligned}$$

■

Match the correct justifications from the following list with the places (a)–(f) where they are needed in the proof.

1. the product rule for probabilities of independent events
2. the product rule for expectations of independent events
3. the product rule for probabilities of disjoint events
4. the sum rule for probabilities of independent events
5. the sum rule for expectations of independent events
6. the sum rule for probabilities of disjoint events
7. the sum rule for expectations of indicator variables
8. definition
9. Chernoff's bound for a sum of index variables
10. inequality $e^x \geq 1 + x$
11. the bounds on the tail of a binomial distribution
12. arithmetic rules for exponents
13. arithmetic rules for $\log_e$

Problem 7. For each of the following pairs of functions $f(n)$ and $g(n)$, fill in the blank with o, O, ω, Ω, and Θ depending on whether $f(n) = o(g(n))$, $f(n) = O(g(n))$, $f(n) = \omega(g(n))$, $f(n) = \Omega(g(n))$, or $f(n) = \Theta(g(n))$. If there is more than one relation between $f(n)$ and $g(n)$, write the strongest one. Suboptimal answers will get partial credit but incorrect answers will be penalized, so do not guess unless you are reasonably sure. As usual, $\lg n$ denotes logarithm to the base 2, and $\lg^2 n$ denotes $(\lg n)^2$.

$$\begin{aligned}
4^{\lg n} &= \underline{\qquad}(n^{1.5}) \\
(2n)! &= \underline{\qquad}(2^n(n!)) \\
n^{(\lg^2 n)} &= \underline{\qquad}\left(2^{\lg^3 n}\right) \\
\binom{2n}{n} &= \underline{\qquad}(n^n) \\
\frac{n^4+n^2+2}{n^2+1} &= \underline{\qquad}\left(\sum_{i=1}^{n} i\right)
\end{aligned}$$

Problem 8. We wish to prove by induction on n that the recurrence

$$T(n) = T(n/2) + T(n/4) + n$$

has an asymptotic growth rate of $O(n)$.

Which of the following induction hypothesis will provide a correct proof? (List all correct answers; more than one may be correct.)

(i) $T(n) \leq 2n$
(ii) $T(n) \leq 4n^2$
(iii) $T(n) \leq 10n$
(iv) $T(n) \leq 4n$
(v) $T(n) \leq 3n + 10$

Answer: ____________________

Problem 9. A lake contains n trout. 100 of them are caught, tagged and returned to the lake. Later another 100 trout are caught, selected independently from the first 100.

(a) Assume that the second 100 trout are selected without replacement. Write an expression (in n) for the exact probability that these trout are found to contain exactly 7 tagged ones.

(b) Now consider selecting the second 100 trout with replacement. That is, you repeat 100 times the following steps: select at random a trout in the lake, check if the trout is tagged and return it to the lake before selecting a new trout.

What is the probability that exactly 7 of the selected trout are tagged?

(c) What is the best way to come up with an estimate of the expression found in part (b) as n becomes large? Select your answer from the following:

1. use Markov inequality
2. use the bound on the tail of the binomial distribution
3. use the central limit theorem
4. use Chebyshev inequality
5. use Poisson approximation

Answer: ____________________

Problem 10. A bridge hand consists of 13 cards. The *suit-distribution* of a hand is the number of cards in each suit. For example, one possible suit-distribution is 4 spades, 3 hearts, 3 diamonds, and 3 clubs.

(a) How many different suit-distributions are there?

(b) How many different suit-distributions are there assuming that you get at least one card in each suit?

(c) Suppose the actual suits don't matter. The *card-distribution* is specified by the *set* of numbers of each suit. In the previous example, the card-distribution would be $\{4, 3, 3, 3\}$. How many card-distributions are possible for a bridge hand? (You need not give a numerical answer, but may use notation from Handout 32 – Notes on Counting.)

Problem 11. Suppose the entries a, b, c, d of a 2×2 matrix

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

are chosen independently at random according to the uniform distribution on $\{0, 1, 2, 3, 4\}$. Let $X = \det(M) = ad - bc$.

(a) What is $E(X)$?

(b) What is $E(X \mid b = 1)$?

(c) What is $Var(X)$?

Problem 12. Find the number of permutations of the letters $\{a, b, c, d, e, f, g\}$ that do not contain "bag" or "def".

Appendix

Problem 5 from Problem Set 4. Let A be a set. Define the set seq(A) to be the set of all finite tuples of one or more elements in A. Namely,

$$\text{seq}(A) = \bigcup_{n>0} \underbrace{A \times \cdots \times A}_{n}.$$

We say a set S is *countable* iff there is an injection from S to $\mathbb{N}$. Prove that seq$(\mathbb{N})$ is countable.

Hint: Define the *norm* of any tuple $\langle n_1, \ldots, n_k \rangle \in \text{seq}(\mathbb{N})$ to be $\max\{k, n_1, \ldots, n_k\}$. Observe that for any $k > 0$, there are only finitely many tuples with norm k.

Proof. Define the *norm* of any tuple $\langle n_1, \ldots, n_k \rangle \in \text{seq}(\mathbb{N})$ to be $\max\{k, n_1, \ldots, n_k\}$. Note that if a tuple t has norm k then t has at most k elements and each element of t is a number between 1 and k (inclusive). Thus for any $k > 0$ there are at most $s_k = k^{k+1}$ tuples with norm k.

Let $N(k) = \{t \mid t \text{ is a tuple with norm } k\}$. Since each $N(k)$ has at most s_k elements we can find injective functions f_1 from $N(1)$ to $\{1, \ldots, s_1 - 1\}$, f_2 from $N(2)$ to $\{s_1, \ldots, s_1 + s_2 - 1\}$ and in general f_n from $N(n)$ to $\{\sum_{i=1}^{n-1} s_i, \ldots, \sum_{i=1}^{n} s_i - 1\}$.

Since $\{N(n)\}_{n>0}$ is a partition of seq$(\mathbb{N})$, we can define a function f from seq$(\mathbb{N})$ to $\mathbb{N}$ by $f(t) = f_n(t)$ where n is the norm of t. Since f maps different $N(n)$'s to disjoint subsets of the integers, and each function f_n is injective on its domain, then f is an injection on the set of all integers.

■

Blank Page