CS 70 Discrete Mathematics and Probability Theory
Spring 2017 Rao

# Midterm 2

PRINT Your Name: ______________________________, ______________________________
(last) (first)

SIGN Your Name: ____________________________________

PRINT Your Student ID: ____________________________________

WRITE THE NAME OF your exam room: ____________________________________

Name of the person sitting to your left: ____________________________________

Name of the person sitting to your right: ____________________________________

- After the exam starts, please *write your student ID (or name) on every odd page* (we will remove the staple when scanning your exam).
- We will not grade anything outside of the space provided for a problem unless we are clearly told in the space provided for the question to look elsewhere.
- The questions vary in difficulty, so if you get stuck on any question, it might help to leave it and try another one.
- **No justifications are needed for True/False or Short Answer questions. Make sure you bubble in or write your answer in the provided box, accordingly.**
- You may consult only *2 sheets of notes*. Apart from that, you may not look at books, notes, etc. Calculators, phones, computers, and other electronic devices are NOT permitted.
- There are **12** single sided pages on the exam. Notify a proctor immediately if a page is missing.
- **You may, without proof, use theorems and lemmas that were proven in the notes and/or in lecture.**
- **You have 120 minutes: there are 5 questions with a total of 43 parts on this exam worth a total of 139 points.**

Do not turn this page until your instructor tells you to do so.

SID:

**1. Modular Arithmetic/RSA** (30 points, 3 points each part)

*Please write your answer in the provided box, or bubble in the corresponding option.*

1. (Short Answer.) Give a number $y$ modulo 35, where $y = 0 \pmod{5}$ and $y = 1 \pmod{7}$.

2. (Short Answer.) Give a number $y$ modulo 35, where $y = 1 \pmod{5}$ and $y = 0 \pmod{7}$.

3. (Short Answer)Give a number $y$ modulo 35, where $y = 4 \pmod{5}$ and $y = 3 \pmod{7}$.

4. (True/False) The public key $d$ is relatively prime to $(p-1)(q-1)$.

○ True

○ False

5. Consider an RSA scheme where $p = 23, q = 5$ and $e = 3$. What is $d$?

6. CRT/FLT/Euler. Recall that the Chinese Remainder Theorem (CRT) implies for distinct primes $p_1, \ldots, p_k$, and $N = p_1 \cdot p_2 \cdots p_k$ that there is a unique $x \in \{0, \ldots, N-1\}$ which is the solution for $x = z_i \mod p_i$, for some $z_1, \ldots, z_k$.

   (a) Say $x = 0$, what is the value of each $z_i = x \pmod{p_i}$?

   (b) Use the CRT to show that the set $S_N = \{x : gcd(x,N) = 1\}$ has size $(p_1 - 1)(p_2 - 1) \cdots (p_k - 1) = \prod_{i=1}^{k}(p_i - 1)$.

   (c) Show that for any $a \in S_N$ that $a^{\prod_{i=1}^{k}(p_i-1)} \equiv 1 \pmod{N}$.

   (d) Assume one chooses $x$ uniformly from $\{0, \ldots, N-1\}$. What is the probability that $x$ is in $S_N$?

   (e) What is the probability that $x$ is in $S_N$ given that $gcd(x, p_1) = 1$?

2. **Countability/Halting** (9 points, 3 for each True/False + 4 points)

   *Please write your answer in the provided box, or bubble in the corresponding option.*

   1. (True/False) For a countable set of strings, some of which have possibly infinite size, the union of all the finite sized substrings of each string is countable. (A substring of a string can be formed by choosing the positions in the original string to include in the substring. Here there will be a finite number of positions.)

      ○ True

      ○ False

   2. (True/False) For any irrational number, there exists a computer program to compute it. (A program computes a number when it outputs any digit at a fixed finite time, even while running perhaps forever. For example, there are programs that compute $\sqrt{2}$ and $\pi$. )

      ○ True

      ○ False

   3. (True/False). Let $f : X \to \mathscr{P}(X)$ be a function from a set $X$ to its power set. True/False: The set $\{x \in X : x \notin f(x)\}$ is not in the range of $f$.

      ○ True

      ○ False

   4. (Argument/Proof.) Let $M$ be a program that takes in a program $P$ and an input $x$, and tells if you some variable $v$ in the program $P$ ever becomes the value 42 when you run $P$ on the input $x$. Prove that such a program $M$ cannot exist.

**3. Polynomial Related Questions.** (24 points, 3 for each part)

*Please write your answer in the provided box, or bubble in the corresponding option.*

In the following, recall that a polynomial, $P(x)$, contains a point $(a,b)$ when $P(a) = b$. And two polynomials, $P(x)$ and $Q(x)$, intersect at a point $(a,b)$ when $P(a) = Q(a) = b$.

1. (Short Answer.) A degree (at most) five polynomial, $P(x)$, intersects a degree (at most) four polynomial, $Q(x)$ at $k$ points. What is the smallest value of $k$ where one can conclude that $Q(x) = P(x)$? (Here your bound should hold for any $P(x)$,$Q(x)$ that obey the degree bound.)

□

2. (Short Answer.) Consider a set of 11 points, and two degree 4 polynomials, $P(x)$ and $Q(x)$, where $P(x)$ contains $k$ points and $Q(x)$ contains a possibly different set of $k$ points. What is the minimum value of $k$ where we can conclude $P(x) = Q(x)$.

□

3. (Short Answer.) Give a degree 2 polynomial modulo 5 that contains $(1,3)$, $(2,0)$, $(3,0)$.

□

4. (Short Answer.) If a channel loses $f$ fraction of packets, how many packets does one need to send to recover a message of length $n$ using polynomial encoding.

□

5. (Short Answer.) If a channel corrupts $f$ fraction of packets, how many packets does one need to send to recover a message of length $n$ using polynomial encoding.

□

6. (Short Answer.) Consider a two variable polynomial $Z(x,y) = P(x)Q(y)$ modulo a prime $p$ where $P(x)$ and $Q(y)$ are nonzero degree $d$ polynomials where $d < p$. What is the maximum number of distinct pairs of $(i, j)$ that satisfy $Z(i, j) = 0 \pmod{p}$.

7. (Short Answer.) Given the error polynomial from Berlekamp-Welsh algorithm, $x^2 + 3x + 2 \pmod{11}$, for what ’$x$’ values are the points corrupted?

8. (True/False.) There exists a bijection between the set of all ordered triples of reals $(a, b, c)$, and the set of polynomials of degree at most 3 that pass through the point (3,3).

○ True

○ False

**4. Counting.** (9 points, 3 for each short answer + 4 points for combinatorial proof)

*Please write your answer in the provided box, or bubble in the corresponding option.*

1. (Short Answer.) What is the number of boy, girl, dog triples from $n$ boys, $m$ girls, and $k$ dogs?

□

2. (Short Answer.) What is the number of different permutations of the letters "SINHOCHEWHI"?

□

3. (Short Answer.) What are the number of ways to divide $m$ dollar bills among $z$ people?

□

4. Give a combinatorial proof that $\binom{k+n-1}{n-1} = \sum_{i=0}^{k} \binom{k-i+n-2}{n-2}$.

5. **Probability** (24 points, 3 for each part 1-8 + 35 points)

*Please write your answer in the provided box, or bubble in the corresponding option.*

In this question $P(\lambda)$ denotes the Poisson distribution with parameter lambda, $B(n,p)$ denotes the Binomial Distribution with parameters $n$ and $p$, $G(p)$ denotes the Geometric Distribution with parameter $p$ and $U\{1,\ldots,n\}$ denotes the uniform distribution over the range $[1,n]$.

1. (True/False) If $Pr[A] > 0$ and $Pr[B] > 0$, and $A$ and $B$ are disjoint then $A$ and $B$ are not independent.

   ○ True

   ○ False

2. (True/False) If $Pr[A|B] = .9$ and $Pr[C|B] = .8$, then $Pr[A] > Pr[C]$?

   ○ True

   ○ False

3. (True/False) For independent $X,Y \sim G(p)$, we have $X+Y \sim G(p/2)$.

   ○ True

   ○ False

4. (True/False) For independent $X,Y \sim P(\lambda)$, we have $X+Y \sim P(2\lambda)$.

   ○ True

   ○ False

5. (True/False) For independent $X,Y \sim B(n,p)$, we have $X+Y \sim B(2n,p)$.

   ○ True

   ○ False

6. (True/False) For independent $X,Y \sim U\{1,\ldots,n\}$ we have $X+Y \sim U\{1,\ldots,2n\}$.

   ○ True

   ○ False

7. (Short Answer) For independent $X \sim B(n,p), Y \sim G(p)$, what is $E[X+Y]$?.

   □

8. (3 points) Find a joint distribution for $X$ and $Y$ such that $X$ and $Y$ are each uniform on the set $\{1,2,3,4,5,6\}$, but $(X,Y)$ is not uniform on $\{1,2,3,4,5,6\} \times \{1,2,3,4,5,6\}$.

9. (Quick Calculation) Let $Z \leq 4$ be a random variable with $\mathbf{E}[Z] = 2$. Give an upper bound for $\Pr(Z \leq 0)$.

10. **Confidence Intervals.** (3 points)

    Consider two shuffled 52-card decks. Let $X$ be the number of cards which are in the same position in both of the decks. Using Chebyshev's Inequality, your friend tells you that $X$ is at least $\alpha$ with probability at most $1/2$. What is $\alpha$?

11. (13 points) Let $X$ be geometric with parameter $p$, $Y$ be Poisson with parameter $\lambda$, and $Z = \max(X,Y)$. For full credit, your final answers should not have summations. (Please try to do all parts using answers from previous ones as necessary.)

    (a) (5 points) Compute $P(Y < X)$.

    (b) (4 points) Compute $P(Z \geq X)$.

    (c) (4 points) Compute $P(Z \leq Y)$.

12. (10 points) You are dealt 13 cards without replacement from a standard 52 card deck. Let $X$ be the number of distinct values in your hand (The 13 possible values are Ace, 2, 3, 4, ..., Jack, Queen, King) ignoring suit. For instance, the hand, again dropping suits, (A, A, A, 2, 3, 4, 4, 5, 7, 9, 10, J, J) has 9 distinct values. (We expect expressions here, no need to simplify your answers or multiply out or anything.)

    (a) (4 points) Calculate $E[X]$.

    (b) (6 points) Calculate $Var[X]$.

13. (6 points) **Testing for cancer.** Let $A$ be the event that a random male has prostate cancer, $B$ be the event that the person tests positive for cancer. Let $Pr[B|A] = .9$, $Pr[B|\overline{A}] = .1$, and $Pr[A] = .1$.

    (a) (3 points) Given a positive test for a random male, what is the probability he has that cancer? (Can leave as an expression with numbers, no need to do the long division.)

    (b) (3 points) If one has prostate cancer, one may or may not die from it. We call death from cancer the event $C$, and say $Pr[C|A] = Pr[C|A \cap B] = .02$. (That is, $C$ is independent of $B$ conditioned on $A$ or in other words the test result doesn't matter so much as the cancer.) If one has surgery, say the probability is $p$ that one dies.
    Say one got a positive test, at what value of $p$ should one not have surgery? In other words, at what value of $p$ is the chance of dying from surgery at least as high as the chance of dying from prostate cancer for someone who tested positive. (Notice $Pr[C|\overline{A}] = 0$ as one can't die from this cancer if one doesn't have it.)