CS 70 Discrete Mathematics and Probability Theory
Fall 2017 Ramchandran and 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. Justify other answers as noted.**
- 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 7 questions with a total of 46 parts on this exam worth a total of 160 points. There are many short answer questions, but some of the "longer" questions are not very challenging so please keep moving.**

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

1. True/False. 9 parts, 3 points each. 27 total. No partial credit. No work necessary.

1. For $x, y > 1$ with $gcd(x, y) = 1$, there is always a pair of integers a, b where $ax + by = 1$ *where* $|b| < x$ and $|a| < y$.

   ◯ True

   ◯ False

2. Suppose $P(n) = n^3$ for every positive integer n and P is a polynomial. Then it necessarily true that $P(x) = x^3$ for all real numbers x.

   ◯ True

   ◯ False

3. Recall that the power set of S, is the set of all subsets of S.Consider a function $f : \mathbb{R} \to \mathscr{P}(\mathbb{R})$ on the reals to its power set. It can be a bijection.

   ◯ True

   ◯ False

   Given a program P, let S_P be the (possibly infinite) set of finite length strings consisting only of 0's and 1's on which P halts.

4. For any program P, S_P is a countable set.

   ◯ True

   ◯ False

5. For any subset, S of the $\{0, 1\}$ strings, there is a program P where $S_P = S$.

   ◯ True

   ◯ False

6. For any events A, B, C in some probability space, $P(A \cap B \cap C) = P(A|B)P(B|C)P(C)$.

   ◯ True

   ◯ False

7. If events A and B are independent, so are $\bar{A}$ and B.

   ◯ True

   ◯ False

8. If events A and B are such that $P(A|B) > P(A)$, then $P(B|A) > P(B)$.

   ◯ True

   ◯ False

9. If event A is independent of itself, then $P(A)$ must be zero.

   ◯ True

   ◯ False

2. Short Answers. 21 parts. 3 points each. 63 total.

No justification needed or looked at. Put answers in box.

1. What is $2^{24} \pmod{35}$?

2. What is the $x \pmod{105}$ where $x = 1 \pmod 3$, $x = 0 \pmod 5$ and $x = 0 \pmod 7$?

3. How many numbers in $\{0, \ldots, 104\}$ are relatively prime to 105?

4. What is $2^{49} \pmod{105}$?

5. What is the multiplicative inverse of 3 modulo 37?

For 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 $P(a) = Q(a) = b$.

6. Recall the secret sharing scheme where the secret is $P(0)$, what is the secret corresponding to a maximum degree 2 polynomial $P(1) = 4 \pmod 5$ and $P(2) = 3 \pmod 5$ and $P(3) = 2 \pmod 5$?

7. Consider sharing an n-bit secret, where the secret is encoded as $P(0)$ for a polynomial of degree k modulo p where s shares will be handed out. How large is p required to be in this setup?

8. Given a degree d polynomial, $P(x)$ that is non-constant, what is the maximum number of times it can take on a value a?

9. Let $P(x)$ and $Q(x)$ be two distinct polynomials (of degree d_p and d_q respectively) which intersect in exactly 4 points. If the lowest degree polynomial that contains those four points has degree 3, what is the minimum value of $d_p + d_q$?

10. How many permutations of ARKANSAS are there?

11. Consider the statements.
    (a) $\mathbb{N} \times \mathbb{N}$ is countable since one can list the set as follows: $(0,0),(0,1),(0,2)...,(1,0),....$
    (b) $\mathbb{N} \times \mathbb{N}$ is countable since one can list the set as follows: $(0,0),(0,1),(1,0),(2,0),(1,1),(0,2)....$

    Which of the above are valid? (a), (b), both, neither.

12. We put n balls in m numbered bins. How many ways are there to do this
    (a) if multiple balls can be placed in the same bin and the balls are distinguishable?

    (b) if each ball is placed in a separate bin and the balls are indistinguishable? (You can assume that $m \geq n$.)

    (c) if the balls are indistinguishable and multiple balls can choose the same bin? That is, we only care how many balls are in each bin.

13. Consider the equation $x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 70$, where each x_i is a non-negative integer.

    (a) How many solutions to this equation are there?

    (b) What if $x_1 \geq 30$ and $x_2 \geq 30$?

    (c) What if $x_1 \geq 30$ or $x_2 \geq 30$? (By or we mean either one or both are greater than 30.)

14. A factory produces a pool of 100 screws that has 5 defective items. You randomly select 10 screws from the pool without replacement. If all 10 screws are not defective, the set is accepted. What is the probability that the set is accepted?

15. You flip a fair coin repeatedly. What is the probability that the first head you see is on the sixth flip?

16. You flip a fair coin repeatedly. What is the probability that the second head you see is on the sixth flip?

17. Suppose 100 people stand in a line, in some random order, where Alice, Bob, and Chris are three of those people. If each permutation is equally likely, what is the probability that Bob is between Alice and Chris but not necessarily standing exactly next to them?

18. Let A, B, C be three events with $P(A) = 0.6, P(B) = 0.6, P(C) = 0.7, P(A \cap B) = 0.3, P(A \cap C) = 0.4, P(B \cap C) = 0.4, P(A \cup B \cup C) = 1$. Find $P(A \cap B \cap C)$.

3. RSA, CRT and Inverses. 20 points.

Show work as asked. Place final answers in boxes, but provide justification where asked, and we may evaluate work outside the box for partial credit.

1. Given an RSA public key pair $(N, e = 3)$, somehow you obtain d. Give an efficient algorithm to find p and q? (Hint: e is 3.)

2. Recall the following statement of the CRT: given k congruencies $x = a_i (\mathrm{mod} n_i)$ where $a_i \neq 0$ and $gcd(n_i, n_j) = 1$ for $i \neq j$, there is exactly one $x (\mathrm{mod} \prod_i n_i)$ that satisfies all k congruencies.

   (a) Consider that all the n_i are prime. Argue in this case that $x^{-1} \pmod{\Pi_i n_i}$ exists.

   (b) Give an example where n_i may not be prime, where x does not have an inverse $\pmod{\Pi_i n_i}$.

   (c) Consider the case where every n_i is prime and we have $y = x^{-1} \pmod{\Pi_i n_i}$. What is $y \pmod{n_i}$?

   (d) Justify your answer above.

4. Longer Polynomial Related Questions. 15 points.

Show work as asked. Place final answers in boxes, but we may look at work.

1. Consider the equation $(a_3x^3 + a_2x^2 + a_1x + a_0)(x^2 + b_1x + b_0) = F(x)(x^2 + b_1x + b_0)$, where $F(x)$ is some arbitrary function.

   (a) Let $F(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ on all but k points. What is the maximum value of k where one can set the values of b_1 and b_0 to ensure that the equation holds for all x? Why?

   (b) For how many values of x must we know $F(x)$ to fully find a_3, a_2, a_1 and a_0, and b_1 and b_0?

2. Alice wants to send Bob a message of n symbols (over $GF(p)$, where p is a prime) over a channel. The channel corrupts each symbol independently with probability q. Alice and Bob decide to use a Reed-Solomon code with Alice sending $(n+m)$ symbols over the channel, and Bob using the Berlekamp-Welch decoding algorithm. If the probability that Bob cannot correctly decode Alice's message is to be kept at most α, then write an inequality (it can involve summations) that solves for the smallest value of m needed for this to be accomplished. (You can leave the equation in raw form but you must clearly express the dependencies on the parameters of the problem.)

5. Finite Diagonalization. 5 points.

1. If I have a set T of k-bit strings, where $|T| = k$, give a procedure that looks at only one bit of each string and constructs a k-bit string that is not in the list. You can do things like let me look at the third bit of string 1, or the first bit of string 5.

6. Counting/Combinatorial Proof. 5 points.

1. Use a combinatorial argument to prove that $\sum_i \binom{n}{i}^2 = \binom{2n}{n}$.

7. Probability. 30 points.

Answers in boxes. Brief justification outside box may be examined.

1. You have n balls numbered $1, \ldots, n$, where n is a positive integer.

   (a) You sample two balls with replacement. What is the probability that the maximum of the two numbers is k, where k is an integer $1 \leq k \leq n$?

   (b) Same question as before, but draw the balls without replacement.

2. You have 5 coins in your pocket. Two of these coins are two-headed (both sides are heads). One coin is two-tailed (both sides are tails). The other two are fair coins. You close your eyes, reach into your pocket and choose one of the coins randomly and flip it.

   (a) What is the probability that the lower face of your tossed coin is a Head?

   (b) You open your eyes and observe that the upper face of your tossed coin is a Head. What is the probability that the lower face is a Head?

   (c) Now you shut your eyes again and toss the same coin. What is the probability that the lower face is a Head?

   (d) You open your eyes again and observe that the upper face is a Head. What is the probability that the lower face is a Head?