CS 70 Discrete Mathematics and Probability Theory
Fall 2017 Ramchandran and Rao Midterm 2 Solutions

PRINT Your Name: Oski Bear

SIGN Your Name: *OSKI*

PRINT Your Student ID: _____

CIRCLE your exam room:
Pimentel 1 GPB 100 Hearst Annex A1 Soda 320 Latimer 120 Other

Name of the person sitting to your left: Papa Bear

Name of the person sitting to your right: Mama Bear

- 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.
- On questions 1-2: You need only give the answer in the format requested (e.g., true/false, an expression, a statement.) We note that an expression may simply be a number or an expression with a relevant variable in it. **For short answer questions, correct clearly identified answers will receive full credit with no justification. Incorrect answers may receive partial credit.**
- On question 3-8, do give arguments, proofs or clear descriptions as requested.
- You may consult one sheet of notes. Apart from that, you may not look at books, notes, etc. Calculators, phones, and computers are not permitted.
- There are **14** 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 8 questions on this exam worth a total of 115 points.**

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

SID:

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 $|a| < y$.

   Answer: True. One can add or subtract the equation $a(-b) + b(a) = 0$, until the too positive or too negative number gets smaller. The other one gets smaller in absolute values as well since any solution has opposite signs.

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.

   Answer: True. Let d be the degree of P. Since $d + 1$ points will uniquely determine the polynomial P, we see that $P(x) = x^3$ because we have infinitely many points on the curve $y = x^3$.

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.

   Answer: False. The power set of the reals is a larger set than the reals. In particular, assume $f : R$ is the bijection, the set of reals $\{x | x \notin f(x)\}$ can't be in the image of the function.

   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.

   Answer: True. It is a subset of the $\{0, 1\}$ strings which is countable.

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

   Answer: False. The powerset of the $\{0, 1\}$ strings is uncountable, the programs are a countable set so there can be no bijection between the two sets.

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

   Answer: False. Experiment is flip two coins, A is two heads, B is first one is heads, C is second is heads. The product would be $1/8$ where $Pr[A] = Pr[A \cap B \cap C] = 1/4$

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

   Answer: True. $Pr[A^c|B] = (1 - Pr[A|B]) = 1 - Pr[A] = Pr[\bar{A}]$

8. If events A and B are such that $P(A|B) > P(A)$, then $P(B|A) > P(B)$. **Answer:** True. $Pr[A \cap B] = Pr[A|B]Pr[B] = Pr[B|A]Pr[A]$, cross divide to get $\frac{Pr[A|B]}{Pr[A]} = \frac{Pr[B|A]}{Pr[B]}$. The assumption is that the left hand side is greater than one, which clearly implies the right hand side is greater than one, which is the consequence of the statement.

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

   Answer: False. Let $Pr[A] = 1$. Then $Pr[A|A] = 1 = Pr[A]$.

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

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

1. What is $2^{24} \pmod{35}$?
   Answer: $1 \pmod{35}$. RSA says $a^{(p-1)(q-1)} = 1 \pmod{35}$.
2. What is the $x \pmod{105}$ where $x = 1 \pmod 3$, $x = 0 \pmod 5$ and $x = 0 \pmod 7$?
   Answer: 70. $5 \times 7 \times (2^{-1} \pmod 3) \pmod{105}$ or 70.
3. How many numbers in $\{0, \ldots, 104\}$ are relatively prime to 105?
   Answer: 48. $(p-1)(q-1)(r-1) = (4)(6)(2)$.
4. What is $2^{49} \pmod{105}$?
   Answer: 2. The modulus is pqr for $p = 5, q = 7$, $r = 3$. We know from homework that $a^{(p-1)(q-1)(r-1)} = 1 \pmod{105}$. Here $(p-1)(q-1)(r-1) = 48$, so we multiply 1 by 2.
5. What is the multiplicative inverse of 3 modulo 37?
   Answer: 25. One can use extended GCD, or see that $3 \times 12 = 36 = -1 \pmod 3 7$, thus multiplying by -12 or 25 gives 1. This is clear in a low depth egcd as well.

   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 $P(3) = 2 \pmod 5$?
   Answer: 0. This is the line $P(x) = -x \pmod 5$
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?
   Answer: The next prime which is at least $\max(2^n, k+1, s+1)$.
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?
   Answer: d times. Otherwise $P(x) - a$ would have more than d roots.
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 $d_p + d_q$?
   Answer: 7. One could have degree 3, the other must be different and there is only one degree 3 polynomial that hits the 4 points, so the sum is 7.
10. How many permutations of ARKANSAS are there?
    Answer: $\frac{8!}{3!2!}$
11. Consider the statements.
    (a) $\mathbb{N} \times \mathbb{N}$ is countable since one can list the set as follows: $(0,0), (0,1), (0,2)..., (1,0), ...$
    Answer: This one is not valid, as one never gets to $(1,0)$.
    (b) $\mathbb{N} \times \mathbb{N}$ is countable since one can list the set as follows: $(0,0), (0,1), (1,0), (2,0), (1,1), (0,2)....$
    Answer: This one is valid.

    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?
    Answer: m^n

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

(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. **Answer:** $\binom{n+m-1}{m-1}$. Stars and bars!

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?
    Answer: $\binom{75}{5}$. This is stars and bars.
    (b) What if $x_1 \geq 30$ and $x_2 \geq 30$? **Answer:** Give x_1 30 balls and x_2 30 balls, so that we are left with 10 balls to arrange into 6 bins and the answer is $\binom{15}{5}$.
    (c) What if $x_1 \geq 30$ or $x_2 \geq 30$? (By or we mean either one or both are greater than 30.)
    Answer: Let A_i be the set of solutions where $x_i \geq 30$. We want $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$ by inclusion-exclusion, hence the solution is $\binom{45}{5} + \binom{45}{5} - \binom{15}{5}$.
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?
    Answer: $\frac{\binom{95}{10}}{\binom{100}{10}}$

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

    Answer: $1/2^6$. You have to see 5 tails and then a heads.

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

    Answer: $\binom{5}{1}(1/2)^6$. You have to have a head somewhere in the first five and a head in the last position. There are $\binom{5}{1}$ such sample points and each has probability $(1/2)^6$.

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?

    Answer: 1/3. The number of people is irrelevant. For each permutation, there are 2 out of 6 ways to sort Alice, Bob, Chris to get the desired result.

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 $P(A \cap B \cap C)$.

    Answer: 0.2

    Inclusion/Exclusion: $P[A \cup B \cup C] = Pr[A] + Pr[B] + Pr[C] - Pr[A \cap B] - Pr[A \cap C] - Pr[B \cap C] + Pr[A \cap B \cap C]$.

    Solve and plug in: $P[A \cap B \cap C] = 1 - 0.6 - 0.6 - 0.7 + 0.3 + 0.4 + 0.4$.

    This works out to 0.2.

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.)

   Answer: $de - 1 = k(p-1)(q-1)$ for $k = 1$ or $k = 2$ or $k = 3$. One can try each to obtain $Y = (p-1)(q-1)$ in at least one of the cases. Then, you have $Y = pq - p - q + 1$ and $pq = N$. Plugging in N/q for p and multiplying through by q into the first equation yields $Yq = Nq - N - q^2 + q$. This is a quadratic equation which one can solve to figure out q. This is similar to the homework problem.

2. Recall the following statement of the CRT: given k congruencies $x = a_i (\text{mod} n_i)$ where $a_i \neq 0$ and $gcd(n_i, n_j) = 1$ for $i \neq j$, there is exactly one $x (\text{mod} \prod_i n_i)$ 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.
   Answer: The solution, x, is relatively prime to $\Pi_i n_i$, since it is relatively prime to each factor.

   (b) Give an example where n_i may not be prime, where x does not have an inverse $\pmod{\Pi_i n_i}$.
   Answer: $x = 2 \pmod 4, x = 1 \pmod 5$.
   Here, $x = 6 \pmod{20}$ and has no inverses since $gcd(6, 20) = 2$.

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

   (d) Justify your answer above.
   Answer: If $x = a_i \pmod{n_i}$ and $y = b_i \pmod{n_i}$, then $xy = a_i b_i \pmod{n_i}$.
   Since $x^{-1}x = 1 + k\Pi_i n_i$, we have $x^{-1}x = x^{-1}a_i = 1 \pmod{n_i}$.
   Since a_i has a unique inverse modulo n_i, then $x^{-1} = a_i^{-1} \pmod{n_i}$.

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?
   Answer: $k = 2$. We can make a quadratic have two zeros and zero out two equations.

   (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?
   Answer: 8. $n + 2k$ where $n = 4$ and $k = 2$ for Welsh-Berlekamp.

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.)

   Answer:
   $\sum_{i>m/2} \binom{n+m}{i} (1-q)^{m+n-i} q^i \leq \alpha$.
   This computes the probability that are more than $m/2$ packets corrupted, and Welsh-Berlekamp succeeds as long as the number of corruptions is less than k where one recieves $n + 2k$ packets. Taking $m = 2k$ we get our result.

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.

   Answer: Build a k bit string by asking for the ith bit of string i, and setting the value of the kth bit to be different from this value.

6. Counting/Combinatorial Proof. 5 points.

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

   Answer: Say we would like to split up a $2n$ large group of people into two teams of equal size. There are $\binom{2n}{n}$ ways to choose teams directly.

   Equivalently, we can temporarily split the $2n$ people into two groups of n people and count the number of ways choose i people from the first group and $n-i$ people from the second group, then sum over all possible values of i. The rest of the people will be on team 2. We note that choosing $n-i$ people from the second group to be on team 1 is the same as choosing i people to not be on team 1; therefore if we count this way we get $\sum_i \binom{n}{i}^2 = \binom{2n}{n}$, and therefore $\sum_i \binom{n}{i}^2 = \binom{2n}{n}$, as desired.

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 $1 \le k \le n$?
   Answer: Let X by the value of the maximum. It is easier to compute $\mathbb{P}(X \le k) = (k/n)^2$. Now the answer follows from $\mathbb{P}(X = k) = \mathbb{P}(X \le k) - \mathbb{P}(X \le k-1) = (k^2 - (k-1)^2)/n^2 = (2k-1)/n^2$.

   (b) Same question as before, but draw the balls without replacement.
   Answer: Note that here $X = 1$ is impossible so assume $k > 1$. There are $n(n-1)$ pairs of balls that can be drawn, and among them if the maximum is $\le k$ then both balls are drawn from $\{1,\ldots,k\}$, so

   $$\mathbb{P}(X \le k) = \frac{k(k-1)}{n(n-1)}.$$

   Now again we have $\mathbb{P}(X = k) = \mathbb{P}(X \le k) - \mathbb{P}(X \le k-1) = [k(k-1) - (k-1)(k-2)]/[n(n-1)] = 2(k-1)/[n(n-1)]$.

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?
   Answer: $6/10$. Each side of a coin is equally likely to be on the bottom by symmetry. Six sides out of 10 are heads, so the bottom side being a head is the ratio.

   (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?
   Answer: $\frac{2}{3}$. The experiment's outcome can be described by coin, side. Each outcome is equally likely. Event A is that the side you see is head. The event B is that the other side is heads. We are asked $Pr[B|A] = Pr[A \cap B]/Pr[A] = (2/5)/(6/10) = 2/3$.

   (c) Now you shut your eyes again and toss the same coin. What is the probability that the lower face is a Head?
   Answer: $5/6$.
   Let B be the event it is a heads-heads coin and A be the event we see a head. Oh. Yeah. We just calculated $Pr[B|A]$ to be $2/3$.
   The total probability of the lower face being a head (let's call the event H) with another flip is $Pr[B]Pr[H|B] + Pr[B^c]Pr[H|B^c] = (2/3) \times 1 + (1/3)(1/2) = 5/6$.

   (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?
   Answer: $\frac{4}{5}$.
   We can update from the previous. Again, the event B corresponds to this being a double heads coin. We let A be the event that we see a head, with the prior already according to the previous part. That is, that $Pr[B] = 2/3$. Now $Pr[A|B] = 1$ and $Pr[A|B^c] = 1/2$.
   And, $Pr[B|A] = Pr[A|B]Pr[B]/Pr[A]$, $Pr[A] = Pr[A|B]Pr[B] + Pr[A|B^c]Pr[B^c] = 5/6$.
   Plugging in we get $Pr[B|A] = 4/5$. Nice! Two-headed coins are more likely!