CS 70 Discrete Mathematics and Probability Theory
Fall 2016 Seshia and Walrand 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 or FALSE?: total 24 points, each part 3 points**
For each of the questions below, answer TRUE or FALSE.
Clearly indicate your correctly formatted answer: this is what is to be graded.No need to justify!

Answer: Note that the answers provide explanations for your understanding, even though no such justification was required

1. If $x \equiv y \pmod{n}$, $z \equiv w \pmod{n}$, and $GCD(z,n) = GCD(w,n) = 1$, then $x \cdot z^{-1} \equiv y \cdot w^{-1} \pmod{n}$, where z^{-1} and w^{-1} are the inverses of z and $w \pmod{n}$.
   Answer: TRUE. z and w both have the same multiplicative inverse mod n.
2. $f(x) = x^5 \pmod{65}$, $x \in \{0,1,\ldots,64\}$, is not a bijection.
   Answer: FALSE. 5 is relatively prime to $(5-1)(13-1)$ making it a valid RSA encryption key, and thus f is a bijection.
3. $11^{97} \pmod{105} = 11$
   Answer: TRUE.
   LHS evaluates to 11. 105 is made up of three primes 3, 5, and 7. By Fermat's Little Theorem, since 11 is coprime, then $11^{(3-1)(5-1)(7-1)} = 11^{48} = 1 \pmod{105}$, therefore $11^{97} = (11^{48})^2 \cdot 11 = (1)^2 \cdot 11 = 11 \pmod{105}$.
4. Polynomial $3x^3 + 5x^2 + 4x + 2$ is perfectly divisible by $x - 3$ (mod 7).
   Answer: TRUE. The result is $3x^2 + 4$.
5. Every infinite subset of the set of real numbers $\mathbb{R}$ is uncountable.
   Answer: FALSE. Consider $\mathbb{N} \subset \mathbb{R}$.
6. There exists a program H that determines whether an arbitrary program P on input x outputs the value of $x+42$ after executing 42 statements.
   Answer: TRUE. H can simply run P and keep track of the "program counter"/location of statements executed in P. If P has executed 42 statements and then prints the value of $x+42$, then it outputs "YES", otherwise "NO".
7. Let p and q be prime numbers, $p \neq q$. Then the number of natural numbers between 1 and pq which are relatively prime to pq is $(p-1)(q-1)$.
   Answer: TRUE.
   There are $q-1$ multiples of p less than pq and $p-1$ multiples of q less than pq. Counting pq itself, there are $(p-1)+(q-1)+1$ numbers less than pq which share a common factor with pq, so the count of numbers which are relatively prime to pq is $pq-(p-1)-(q-1)-1 = (p-1)(q-1)$.
8. Professor Random has graded 100 exams and all scores are distinct. In class, she shuffles the exams and begins reading the scores aloud. Let A_k be the event that the kth exam score she reads is the top score so far. Then A_k and A_{k+1} are not independent.
   Answer: FALSE.
   Consider the first k exams, and let E_k be the highest-scoring exam out of the first k exams. The event A_k is the event that E_k is located at the kth position in the pile of exams. Since the exams were shuffled beforehand, E_k is equally likely to be found in any of the first k positions, so $\Pr[A_k] = 1/k$. Similarly, $\Pr[A_{k+1}] = 1/(k+1)$. To compute $\Pr[A_k \cap A_{k+1}]$, observe that there are $(k+1)!$ total permutations of the first $k+1$ exams. $A_k \cap A_{k+1}$ is the event that E_k is in the kth position and E_{k+1} is in the $(k+1)$th position. Once we fix those positions, there are $(k-1)!$ permutations satisfying these constraints. Hence, $\Pr[A_k \cap A_{k+1}] = (k-1)!/(k+1)! = (1/k)(1/(k+1)) = \Pr[A_k]\Pr[A_{k+1}]$.

2. Short Answers: 5x3=15 points Clearly indicate your correctly formatted answer: this is what is to be graded.No need to justify!

1. You roll a balanced six-sided die three times. What is the probability that there are exactly two dice whose sum is 11?

   Answer: For exactly two dice to sum to 11, we need to roll a 6, a 5, and some value $x \in \{1,2,3,4\}$, in any order. There are $3 \times 2 = 6$ ways to permute 6, 5, and x. There are 4 options for x in each of these orderings. Therefore the probability is $\frac{6 \cdot 4}{6^3}$ since there are 6^3 equally likely outcomes of the three dice rolls.

2. How many combinations of even natural numbers (x_1, x_2, x_3, x_4) are there such that $x_1 + x_2 + x_3 + x_4 = 20$?

   Answer: (13 choose 3). Stars and bars. Instead of 20 stars, use 10 stars (now each star represents 2). Another way is to think of each $x_i = 2y_i$ and count the number of y_is that add to 10.

3. Astronomers at the University of Infinity have determined that there are countably infinite stars, and they have given each one a unique identifier in $\mathbb{N}$ defined by the function: id : Stars $\to \mathbb{N}$. Then, one day, they discover a new star s and add it to Stars. How can they set $id(s)$ to be distinct from all the other identifiers?

   Answer: Consider $f = id^{-1}$. Set $f(n) = f(n+1)$ for all n, and $f(0) = s$. That is, remap nth ID to $n+1$, and give the new star the ID 0.

4. The standard polynomial secret sharing is being used and we are working mod 5. Three shares are required to determine the secret, encoded as $P(0)$. We have the following shares: $P(1) = 2, P(2) = 0, P(3) = 2$. What is the secret?

   Answer: The secret is 3.

   Let $P(x) = a_2x^2 + a_1x + a_0$.

   From the shares, we get the following set of equations:

$$\begin{aligned} a_2 + a_1 + a_0 &= 2 \\ 4a_2 + 2a_1 + a_0 &= 0 \\ 9a_2 + 3a_1 + a_0 &= 2 \end{aligned}$$

   Solving, we get $P(x) = 2x^2 + 2x + 3$.

5. Suppose $x = 4 \pmod 7$ and $x = 7 \pmod{11}$. What is $x \pmod{77}$?

   Answer: The answer is 18. Start listing the numbers which equal 7, modulo 11: $7, 18, 29, \ldots$. Out of these numbers, observe that $18 \equiv 4 \pmod 7$ so it satisfies the first equation as well. By the Chinese Remainder Theorem, this is the unique solution. (The Chinese Remainder Theorem was not necessary to solve this question, but it provides the justification that the solution is unique.)

3. Short Proofs: 4+4+4+4+4=20 points

1. Let $r^2 = 1 \pmod{n}$. Show that, if $GCD(r-1,n) = 1$, then $r = n-1 \pmod{n}$.
   Answer: $1 = gcd(r-1,N)$
   $1 = (r-1)u + Nv$
   Multiply both sides by $r+1$
   $r+1 = (r^2-1)u + N(r+1)v$
   We know that $r^2 - 1 = 0 \pmod{N}$.
   So $r+1 = 0(modN)$ or $r = -1(modN)$.
2. Let $x_1, x_2, \ldots, x_n$ be n integers, and p be a prime number. Show that:
   $(x_1 + x_2 + \ldots + x_n)^p = x_1^p + x_2^p + \ldots + x_n^p \pmod{p}$.
   Answer: We know that $a^p = a \pmod{p}$ from Fermat's Little Theorem (and the special case of $a = 0$). Thus, $(x_1 + x_2 + \ldots + x_n)^p = (x_1 + x_2 \ldots + x_n) \pmod{p}$. Also $x_i^p = x_i \pmod{p}$, so the RHS is also equal to $(x_1 + x_2 \ldots + x_n) \pmod{p}$.
3. Consider the function `is_mod_2` below which takes as input an arbitrary program `P`:

```
def is_mod_2(P):
 if (P implements the mod 2 function) then
   return TRUE
 else
   return FALSE
```

   Prove that `is_mod_2` cannot exist.
   Answer:
   Reduce the halting problem to is_mod_2.

```
def halt(P, x):
__def t(n):
_____P(x)
_____return n%2
__return is_mod_2(t)
```

   In other words, t be a function that returns mod 2 correctly if P halts on x.

4. Assume $a > b \geq 1$ where $a, b \in \mathbb{N}$. Prove $\sum_{k=b}^{a} \binom{k}{b} = \binom{a+1}{b+1}$.

   Answer: RHS: Pick $b+1$ representatives from a line of $a+1$ candidates. LHS: Pick all $b+1$ representatives from only the first $k+1$ candidates in the line. This means the last representative is at position $k+1$, and the remaining b representatives must be picked from the first k positions. k has a minimum value of b, since you can't pick b representatives from less than k choices. k has a maximum value of a, since there are only $a+1$ candidates. We sum over all possible values of k.

5. Suppose $P(B|A) = P(B|\bar{A})$ where $\bar{A}$ is the complement of A. Prove that it must be the case that B is independent of A.

   Answer: Let $P(B|A) = P(B|\bar{A}) = p$. One has

$$\begin{aligned} P(B) &= P(A \cap B) + P(\bar{A} \cap B) \\ &= P(B|A) \cdot P(A) + P(B|\bar{A}) \cdot P(\bar{A}) \\ &= p \cdot (P(A) + P(\bar{A})) = p \end{aligned}$$

4. Checking Work:3+3= 6 points

Each of the parts below has some work (proof, reasoning, computation, etc.) that you must check. State the *first error* you find, and explain your answer briefly.

1. Suppose Alice wishes to send Bob a confidential message using RSA. For this, Bob must first set up his public-private key pair. Below, we show the choices Bob made in picking his keys, where he makes at least one mistake.

   Suppose that Bob chooses primes $p = 7$, $q = 13$. (Assume these are large enough.)

   He computes $N = pq = 91$.

   Then Bob chooses $e = 3$ so his public key is $(3, 91)$.

   Finally Bob chooses $d = 61$ which is his private key.

   □

   Answer: The choice of e is incorrect. $(p-1)(q-1) = 72$ and $GCD(3,72) \neq 1$.

2. Proposition: Consider a set of n identical aliens who each want to pick a single color for their T-shirt from a set of k colors. Then the number of ways of assigning colors to the aliens is $\frac{k^n}{k!}$.

   Proof: The first alien picks a T-shirt color in k ways.

   Same for the second, third, etc. So total k^n ways.

   But these aliens are all identical, so we divide by the number of orderings of the k colors, which is $k!$.

   This yields the desired answer. □

   Answer: Last but one line is wrong.

   Second rule does not apply as discussed in class. Need to use the "stars and bars" technique instead.

5. Sharing RSA Keys: 5+5+5=15 points

Consider a set of n people connected on a broadcast network: that is, any message sent by one person intended for another can be received by all. Further, assume that there is exactly one malicious person on this network, named Eve.

Recall that RSA provides Alice a secure way of sending a message to Bob provided that she knows Bob's public key. But how does Alice get to know Bob's public key in the first place? She could send a message to Bob asking him for it, but what if Eve pretends to be Bob and sends her the wrong key?

To deal with this problem, Alice decides to design a new protocol based on the secret sharing scheme studied in class. The general idea is that Bob will send a piece of his public key to everyone, including Eve. If at least k of those people get together, they can reconstruct Bob's key. Otherwise, they cannot.

Answer the following questions:

(a) Recall that the public key is of the form (N,e), where $N = pq$. Design a polynomial $P(x)$ that Bob can use to share his public key using the protocol Alice designed.

Answer: We pick a polynomial $P(x)$ of degree $k-1$ where N and e are two of the coefficients, say a_0 and a_1, and all other coefficients are chosen randomly. Further, we work mod r where r is the first prime larger than N.

(b) Now suppose Alice broadcasts a request for Bob's public key and gets back exactly $k-1$ numbers. Can Alice always recover Bob's public key? Why or why not?

Answer: Not always. Together with her share, Alice now has k numbers. But consider what happens if Eve is one of the k and modifies her share arbitrarily. Then, Alice will end up reconstructing a different polynomial with possibly different coefficients a_1 and a_0, i.e., with a different public key.

(c) At least how many numbers must Alice get back to be able to completely reconstruct the public key? Justify.

Answer: She needs at least $k+1$.

Alice has one share (her own) that she knows to be correct. She needs to get $k-1$ more. Eve's action is like corrupting a packet. So we can apply Reed-Solomon codes and determine that Alice needs to get shares from at least $(k-1)+2 = k+1$ people (since there is at most one corruption, and she needs to get $k-1$ correct numbers). Alice can then use Berlekamp-Welch decoding for the remaining to recover the $k-1$ numbers, and thus the secret coefficients and the public key.

6. Correcting Errors that Grow: 5+5=10 points

Consider a communication channel that *slowly degrades* over time. Specifically, it behaves as follows: Of the first n packets, it drops none; of the second n packets, it drops 1 (but you don't know which one); of the third set of n, it drops some 2; and so on, until for the $n+1$th set of n packets (and thereafter), it drops all of them.

In the questions below, a message is the cumulative sequence of packets transmitted over the channel over all time. Justify all answers, supplying a proof where needed.

(a) Suppose the channel does not corrupt any packets. What is the maximum size, if any, of a message that you can transmit through this channel using the Erasure code you studied in class?

Answer: If you want to transmit a message of length m in a channel with k erasures, you need to transmit $m+k$. So set $m+k=n$ for $k=0,1,\ldots,n$. Then $m=n,n-1,n-2,\ldots,0$. Thus, the message can be at most $n+(n-1)+(n-2)+\ldots+1=\frac{n(n+1)}{2}$.

(b) Now suppose that the channel does not drop packets, but corrupts packets as above — i.e., corrupts none of the first n, an arbitrary one of the next n, etc. What is the maximum size message you can transmit successfully using Reed-Solomon codes and Berlekamp-Welch decoding?

Answer: Recall that if you want to transmit a message of length m in a channel with k corruptions, you need to transmit $m+2k$. So set $m+2k=n$ for $k=0,1,\ldots,n$. Then $m=n,n-2,n-4,\ldots,0$.

If we assume n is even, then message can be at most $n+(n-2)+(n-4)+\ldots+(n-2\frac{n}{2})$ which is $[n+(n-1)+(n-2)+\ldots+\frac{n/2}{\rceil}-\sum_{i=1}^{n/2} i$ or $(\sum_{i=1}^{n} i)-(\sum_{j=1}^{n/2-1} j)-(\sum_{i=1}^{n/2} i)$.

If n is odd, then $m=n,n-2,n-4,\ldots,1$, so 1 more.

7. Countability: 5+5=10 points

Let S be the power set of $\mathbb{E}$, the set of all *even* natural numbers. Let T be the set of functions that map $\mathbb{E}$ to $\{0,1\}$.

(a) Prove that there exists a bijection between S and T.

Answer: Since each element $s \in S$ is a subset of the $\mathbb{E}$, we can express s as a function $f_s(n)$ that evaluates to 1 if $n \in s$ and evaluates to 0 if $n \notin s$. This is a function that maps $\mathbb{E}$ to $\{0,1\}$.

The mapping of s to f_s is one-to-one since if $s_1 \neq s_2$, then f_{s_1} differs from f_{s_2} for the element in the symmetric difference of s_1 and s_2.

It is onto as every function f_s mapping $\mathbb{E}$ to $\{0,1\}$ has a corresponding set s – the set of all n that are mapped to 1.

(b) Is S countable? Justify your answer.

Answer: No, each function mapping $\mathbb{E}$ to $\{0,1\}$ can be expressed as a real number between 0 and 1, as the concatenation $f(0), f(2), f(4), \ldots$. Thus T and therefore S are uncountable, since $\mathbb{R}[0,1]$ is uncountable.

8. Line up for Class, Randomly: 3+3+3+6=15 points

There is a class with $2n$ children where n are boys and n are girls. They have to stand in a line to go to class. Assume that all possible ways in which they might line up are equally likely.

Answer the following questions. *Justify/prove your answer in all cases.*

(a) What is the probability that they alternate by gender?

Answer: $\frac{2 \cdot n! \cdot n!}{2n!}$ There are $n! \cdot n!$ possibilities for them to line up alternating with a girl first, and $n! \cdot n!$ possibilities for them to line up alternating with a boy first. These are disjoint events so you can add together those countings.

(b) What is the probability that all of the girls are before all of the boys?

Answer: $\frac{n! \cdot n!}{2n!}$ There are $n!$ ways for the girls to line up first and then $n!$ ways for the boys to line up behind them, and a total of $2n!$ ways for them to all line up.

(c) What is the probability that between any two girls there are no boys (i.e. that all of the girls stand together in an uninterrupted block)?

Answer: $\frac{(n+1)\cdot n!\cdot n!}{2n!}$ There are $n+1$ locations that the first girl can stand (positions 1 through $n+1$ in the line), and then there are $n!$ ways for the girls to line up in their block, and then $n!$ ways for the boys to line up in the remaining locations.

(d) What is the probability that neither the boys nor the girls stand together in an uninterrupted block?

Answer: Let B be the event that the boys are in a contiguous block, and let G be the event that the girls are standing in a contiguous block. We want to find $Pr[\overline{B}\cap\overline{G}]$ which is equivalent to:

$$\begin{aligned} Pr[\overline{B}\cap\overline{G}] &= Pr[\overline{B\cup G}] \\ &= 1 - Pr[B\cup G] \\ &= 1 - (Pr[B] + Pr[G] - Pr[B\cap G]) \end{aligned}$$

From part (c) we have that $Pr[B] = Pr[G] = \frac{(n+1)\cdot n!\cdot n!}{2n!}$. To get $Pr[B\cap G]$, we know that there are $\frac{n!\cdot n!}{2n!}$ ways for the girls to all line up before the boys, so there are also $\frac{n!\cdot n!}{2n!}$ ways for the boys to line up before the girls, so $Pr[B\cap G] = \frac{2\cdot n!\cdot n!}{2n!}$. Thus,

$$\begin{aligned} Pr[\overline{B}\cap\overline{G}] &= 1 - \left(\frac{(n+1)\cdot n!\cdot n!}{2n!} + \frac{(n+1)\cdot n!\cdot n!}{2n!} - \frac{2\cdot n!\cdot n!}{2n!}\right) \\ &= 1 - \frac{(2(n+1)-2)\cdot n!\cdot n!}{2n!} \\ &= 1 - \frac{2n\cdot n!\cdot n!}{2n!} \\ &= 1 - \frac{n!\cdot n!}{(2n-1)!} \end{aligned}$$

(Scratch space)