EECS 70 Discrete Mathematics and Probability Theory
Spring 2013 Anant Sahai MT 2

PRINT your student ID: _____

PRINT AND SIGN your name: _____, _____ _____
(last) (first) (signature)

PRINT your Unix account login: cs70-_____
PRINT where you are taking this exam: _____
PRINT your discussion section and GSI: (where you want it back) _____

Mark Here	Section	Time	Location	GSI
	1	9-10am	6 Evans	Ramtin
	2	10-11am	71 Evans	Ramtin
	3	11-12pm	71 Evans	Nima
	4	12-1pm	2 Evans	Nima
	5	1-2pm	87 Evans	Sridhar
	6	2-3pm	2070 VLSB	Sridhar
	7	3-4pm	85 Evans	Chung-Wei
	8	4-5pm	9 Evans	Chung-Wei
	9	5-6pm	9 Evans	Richard
	10	1-2pm	3105 Etch.	Chenyu
	11	2-3pm	151 Barr.	Kate
	12	4-5pm	B51 Hilde.	Richard
	13	6-7pm	70 Evans	Sibi
	14	12-1pm	101 Wheel.	Chenyu
	15	4-5pm	156 Dwin.	Sibi

Prob. 1	
Prob. 2	
Prob. 3	
Prob. 4	
Total	

Names of the people sitting next to you: _____

You may consult your two handwritten note sheets. **(You must turn them in with your exam, along with any scratch paper you might have used. Your name and SID should be on each sheet of paper.)** Phones, calculators, tablets, and computers are not permitted. No collaboration is allowed at all and you are not allowed to look at another's work.

Please write your answers in the spaces provided in the test; in particular, we will not grade anything on the back of an exam page unless we are clearly told on the front of the page to look there.

You have 120 minutes. There are 4 questions, of varying numbers of points. The questions are of varying difficulty, so avoid spending too long on any one question.

PRINT your name and student ID: _____

SOME APPROXIMATIONS AND OTHER USEFUL TRICKS THAT MAY OR MAY NOT COME IN HANDY:

$$n! \approx \sqrt{2\pi n}(\frac{n}{e})^n$$

$$\binom{n}{k} \leq (\frac{ne}{k})^k$$

When x is small, $\ln(1+x) \approx x$

When x is small, $(1+x)^n \approx 1+nx$

$$\lim_{n\to\infty}(1+\frac{x}{n})^n = e^x$$

You probably have others on your note sheet and in your minds. Good for you.

The Golden Rule of 70 (and Engineering generally) applies: if you can't solve the problem in front of you, state and solve a simpler one that captures at least some of its essence. You'll get partial credit for doing so, and maybe you'll find yourself on a path to the solution.

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

PRINT your name and student ID: _____

Problem 1. Secret Sharing (15 points)

Suppose that N is the secret number, and is restricted to be one of $0,1,2,3,4$.

A person decides to divide this secret into four shares by using the following K,L secret sharing scheme. (He has kept the identity of K and L hidden from the people he is sharing the secret with.)

To person i, where i is either $1,2,3$, or 4, he gives the share $S_i = (N + K * i + L * i * i) \bmod 5$.

a. 5 points Suppose that three individuals had the following shares: $S_1 = 2, S_2 = 0, S_3 = 2$. **Calculate the secret N and show your work.**

b. 10 points Now suppose that the people learn the method by which the secret N and the keys K, L were generated:

First, he rolls a 5-sided fair die (labeled 0,1,2,3,4) and calls the first number K.

Then, he rolls a 5-sided fair die (labeled 0,1,2,3,4) and calls the second number L.

Finally, he rolls a 4-sided fair die (labeled 0,1,2,3) and calls the third number N. (So they already know it can't be 4.)

Prove that the event $\{N = 2\}$ is independent of the event $\{S_1 = 2, S_2 = 0\}$.

PRINT your name and student ID: _____

Extra Page

PRINT your name and student ID: _____

Problem 2. Counting your ABCs (20 points)

a. (8 points) **How many strings of length $4n$ are there that have exactly n letter 'a's, n letter 'b's, and $2n$ letter 'c's?**

b. (12 points) **Use Stirling's approximation to estimate how fast the answer to the previous part grows as a function of n. Is it essentially exponential in n? If so, it is like what to the nth power?**

PRINT your name and student ID: _____

Extra Page

Problem 3. [True or false] (24 points)

Circle TRUE or FALSE.

Prove all statements that you think are true and disprove (e.g. by showing a counterexample) all statements that you think are false.

Reminder: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ represents the set of non-negative integers.

(a) TRUE or FALSE: If $0 < P(A) < P(B) < 1$, then $P(A|B) < P(B)$.

(b) TRUE or FALSE: If $P(A) = \frac{1}{4}$ and $P(B) = \frac{1}{3}$ and $P(A \cup B) = \frac{1}{2}$, then A and B are independent.

(c) TRUE or FALSE: Let $f_k(x)$ be a real polynomial of degree k that takes the value 1 at $x = k$ and takes the value 0 for $x = 0, 1, \ldots, k-1$. Then, $f_k(x)$ must take non-negative integer values at all non-negative integers x.

PRINT your name and student ID: _____

[Extra Page]

PRINT your name and student ID: _____

Problem 4. Orpheus' Adventures in the Halls of Time (55 points)

You're designing a new role-playing game for a mathematically themed production house. Your eccentric colleague comes to you with an idea for a key scene and he wants you to think about it.

The backstory is that the mortal Orpheus wants to gain knowledge of the dates of certain key events in the year to come: call these the prophecies of interest. He has heard that in the Halls of Time, these things are already known so he quests through the underworld till he comes upon them.

In the Halls of Time, he encounters the Guardians. They have access to the knowledge of the Fates.

a. (20 points) On the medium difficulty setting, the game behaves as follows. There are 12 guardians (corresponding to the 12 constellations of the Zodiac or the 12 months) and each knows all the prophecies, but they have a peculiar property. Half of them are honest and answer questions posed to them exactly. One quarter of them consider mortals to be beneath them and will simply say "Begone mortal!" And one quarter despise mortals and will answer maliciously.

But mortals do not know the secret forms of the guardians and so Orpheus doesn't know who he is talking to.

On this setting, Orpheus can only ask questions (he can invoke arithmetic operations in $GF(367)$ if he wants) whose answer is a number from $\{0,1,2,\ldots,366\}$.

(Hint: You can ask them to encode a prophecy of interest as follows: 1, ..., 365 for the days in the coming year. 0 for the past. 366 to represent the future beyond this coming year. Fortunately for Orpheus, 367 happens to be prime.)

(The prophecies he wants are answers to questions like: "When will my wife die?" Using the above hint, these can be viewed as numbers.)

He can only ask any individual guardian one question. After that, that particular guardian will magically leave the room. He gets to question all 12 guardians.

How many prophecies can Orpheus reliably extract from the 12 guardians? How can he do it? (Be explicit) Why will this work?

PRINT your name and student ID: _____

[Extra Page.]

b. (5 points) Your friend comes to you with a further twist for the hard-mode of the game. He says that one-quarter (3) of the guardians are lazy instead of being honest. Each lazy guardian just randomly chooses one of its sibling guardians and telepathically asks them how they would answer this particular question. (If it happens to choose another lazy guardian, that guardian will again telepathically ask a random sibling until someone answers or would say "begone.") Once it gets some answer telepathically, the lazy guardian being questioned simply repeats that answer out loud and leaves the room. (Telepathic conversations don't cause guardians to leave the room, only speaking an answer out loud.)

If we choose one of the 12 guardians uniformly at random to query, what is the probability that we get a malicious answer?

c. (10 points) Using the setup from part (b) but asking questions of all 12 guardians, **if Orpheus only wants to extract a single prophecy, how should Orpheus proceed and what is his probability of being successful?**

PRINT your name and student ID: _____

[Extra Page.]

d. (20 points) On the easy difficulty setting, the game is quite different. There are just 400 guards and they don't know much. They can carry prophecy books, each containing one prophecy. But the Fates have scattered 200 distinct books of prophecy across them by assigning each prophecy at random (by rolling a fair 400-sided die) to one of the guards. The guards carry their books and because Orpheus can only get the prophecies from one guard, he finds the one who is carrying the most and asks her for everything she is carrying.

Orpheus knows that the guard will demand 1 chicken for every prophecy book that she carries. **How many chickens should Orpheus carry with him so that he has at least about a fifty percent chance of being able to get all the prophecy books carried by that guard?** (Try not to have Orpheus carry too many chickens if you can.)

PRINT your name and student ID: _____

[Extra Page.]