Study Guide and Sample Problems for Midterm 2

This study guide gives some of the important points you should know well before the midterm. It is not a comprehensive list, but if you understand everything on this list you should do well on the midterm.

Polynomials, Secret Sharing and Error-correcting Codes:

- The basic property of polynomials modulo a prime, that any polynomial of degree d is uniquely determined by its value at $d+1$ points.
- The procedure for reconstructing a polynomial of degree d given its values at $d+1$ points.
- The number of polynomials of degree d that go through $d-k$ points.

Once you have understood the basics, you should also review the scheme for secret sharing and error correcting codes. What are the conditions under which they work.

1. You are given three points, $(0,2),(1,7)$ and $(2,1)$. What is the probability that a degree 5 polynomial in GF_{11}, with coefficients chosen uniformly at random, passes through these three points?
2. Given the same three points, what is the probability that a degree 1 polynomial in GF_{11}, with coefficients chosen uniformly at random, passes through these three points?
3. Find the degree 2 polynomial over Z_7, that passes through $(0,1),(1,3),(2,0)$.
4. (a) (5 pts) A function $f(x)$ on GF_p returns a value in GF_p given any input $x \in GF_p$. Two functions f and g are *distinct* if there is some value x for which $f(x) \neq g(x)$. How many distinct functions are there on GF_p?

   (b) Any polynomial on GF_p can be written as
   $$q(x) = a_{p-1}x^{p-1} + a_{p2}x^{p-2} + \cdots + a_0$$
   where the coefficients $a_{p-1}, \ldots, a_0$ must also be in GF_p. Two such polynomials are *apparently distinct* if they have different coefficients. How many apparently distinct polynomials are there on GF_p?

   (c) Prove that if two polynomials $q(x)$ and $r(x)$ on GF_p are apparently distinct then they are distinct functions.

(d) Hence show that every function on GF_p is also a polynomial on GF_p. (Note: Lagrange interpolation is a constructive proof of this fact, but we are not asking for a constructive proof in this problem.)

5. Suppose you use a polynomial $p(x)$ of degree 5 over the field Z_{13} as your error-correcting code (to encode the message $p(0)$). You happen to know that you correctly received the values $p(1), p(2), p(3), p(10), p(11)$, but all the remaining values were corrupted during transmission. Can you recover the message $p(0)$? How?

6. Consider a transmission of the polynomial encoding, where errors occur at points 0, 1, and 2. What is the error polynomial as defined in our lecture on Berlekamp-Welsh?

Eulerian Graphs:

This is straightforward. You should know what it means for a graph to be Eulerian and necessary and sufficient conditions.

1. Prove that if a town has only two way streets, where any street can be reached from any other, then it is possible to traverse each street exactly once in each direction and return to the starting point.

2. (True/False) The complete graph on n nodes is the graph where every pair of nodes is an edge. The complete graph on n nodes is Eulerian for n odd.

Counting:

- The first and second rules of counting.
- Number of ways of placing balls in bins, with and without replacement.
- n choose k.

Once you are clear about the basics, you should also review combinatorial proofs.

1. Youve been hired by the local phone company. Theyre concerned, because all the local taxi companies have started demanding phone numbers made up of exactly 2 different digits. (For instance, "555-5556" and "811-1881" are acceptable, but "111-1111" and "123-4567"

are not.) Your job is to help the phone company figure out how long theyve got before they run out of acceptable phone numbers.

How many 7-digit numbers are there that contain exactly 2 different digits?

2. What is the number of ways to pick n fruits from k varieties of fruits.

3. Give a combinatorial proof of the identity

$$\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}$$

Discrete Probability:

- Clear understanding of sample space, sample point, event.
- Definition of conditional probability (recall the figure that goes with it).
- Bayes rule.
- Independent events.

1. Alice flips a fair coin n times in a row. What is the probability that she receives exactly i heads?

2. At a parking lot there are 12 parking spaces in a row and 8 cars parked in them. What is the probability that there are 4 empty spaces in a row?

3. Suppose of the numbers $1, 2, 3, 4, 5$ we first pick one number and then a second out of the remaining four. What is the probability that the second one picked is odd? What is the probability that both the first and the second are odd?

4. Each of the 50 states has two US senators. A committee of 20 senators is chosen uniformly at random from among all 100 senators. Answer the following questions, justifying each answer carefully:

   (a) What is the sample space, and what is the probability of each sample point? [Your answer may contain binomial coefficients of the form $\binom{x}{y}$.]

(b) Let CC be the event that the committee includes both of the senators from California. What is the probability of CC? [Your answer should be expressed as a rational number in reduced form.]

(c) Let W be the event that the committee contains at least one senator from Wyoming. What is the conditional probability of CC given W? [Your answer should be expressed as a rational number in reduced form.]

(d) Are CC and W independent events? Remember to justify your answer.

(e) What is the probability that at least one state has two members in the committee? [Your answer may contain binomial coefficients of the form $\binom{x}{y}$.]

5. A biased coin with $\Pr[heads] = p$ and $\Pr[tails] = q$ is tossed N times ($N > 0$). Let the probability of an even number of heads after N tosses be A_N and the probability of an odd number of heads after N tosses be B_N.

   Show by induction that

   $$B_N - A_N = (p - q)^N$$

6. Suppose $\frac{1}{5}$ of all men are colorblind and $\frac{1}{3}$ of all women are colorblind. Assume we pick a person uniformly at random from a room with 25 men and 75 women and the person turns out to be colorblind. What is the probability the colorblind person is male?

7. Suppose you are given a bag containing n unbiased coins. You are told that $n - 1$ of these are normal coins, with heads on one side and tails on the other; however, the remaining coin has heads on both its sides.

   (a) Suppose you reach into the bag, pick out a coin uniformly at random, flip it and get a head. What is the (conditional) probability that this coin you chose is the fake (i.e., double-headed) coin?

   (b) Suppose you flip the coin k times after picking it (instead of just once) and see k heads. What is now the conditional probability that you picked the fake coin?

   (c) Suppose you wanted to decide whether the chosen coin was fake by flipping it k times; the decision procedure returns FAKE if all k flips come up heads, otherwise it returns NORMAL. What is the (unconditional) probability that this procedure makes an error?