CS 70 Discrete Mathematics and Probability Theory
Summer 2015 Chung-Wei Lin HW 3

Due Monday July 13 at Noon

1. **Polynomials and Fields** (25 points, 5 points for each part)

   Assume $p(x) = 2x+3$, $q(x) = -x-3$, and $r(x) = -2x$ for the following parts.

   (a) Find all values of the polynomials in mod 4 using the table below. Where do p and q intersect? Where do p and r intersect?

x	$p(x)$	$q(x)$	$r(x)$
0			
1			
2			
3			

   (b) Do Part (a) in mod 5.

x	$p(x)$	$q(x)$	$r(x)$
0			
1			
2			
3			
4			

   (c) Do Part (a) in mod 6.

x	$p(x)$	$q(x)$	$r(x)$
0			
1			
2			
3			
4			
5			

   (d) Where do p and q intersect in $\mathbb{R}$ and $\mathbb{Q}$? Where do p and r intersect in $\mathbb{R}$ and $\mathbb{Q}$? Referring back to Parts (a), (b), and (c), which case is most similar to $\mathbb{R}$ and $\mathbb{Q}$ in terms of the numbers of intersections between polynomials?

   (e) We always considered $(xy = 0) \implies (x = 0) \vee (y = 0)$ to be true in $\mathbb{R}$ and $\mathbb{Q}$. Prove (if true) or provide a counterexample (if false) for the following statements:

   $$(xy \equiv 0 \pmod 4) \implies (x \equiv 0 \pmod 4) \vee (y \equiv 0 \pmod 4);$$
   $$(xy \equiv 0 \pmod 5) \implies (x \equiv 0 \pmod 5) \vee (y \equiv 0 \pmod 5);$$
   $$(xy \equiv 0 \pmod 6) \implies (x \equiv 0 \pmod 6) \vee (y \equiv 0 \pmod 6).$$

   Restate which case is most similar to $\mathbb{R}$ and $\mathbb{Q}$?

2. **More Points (for Polynomials)!** (25 points, 5 points for each part)

   (a) Given 3 points $(0,1)$, $(1,1)$, and $(2,3)$, use Lagrange interpolation to construct the degree-2 polynomial going through these points.

   (b) Given 4 points $(0,1)$, $(1,1)$, $(2,3)$, and $(-1,3)$, does there exist a degree-2 polynomial going through these points? If yes, find the polynomial; if no, explain why none exists.

   (c) Given 4 points $(0,1)$, $(1,1)$, $(2,3)$, and $(-1,0)$, does there exist a degree-2 polynomial going through these points? If yes, find the polynomial; if no, explain why none exists.

   (d) Design a machine (*i.e.*, give the pseudocode for an algorithm) with the following function: Given 4 points $(x_1,y_1),(x_2,y_2),(x_3,y_3),(x_4,y_4)$ with all x_i distinct, the machine outputs `TRUE` if there exists a polynomial $p(x)$ of degree at most 2 such that $p(x_i) = y_i$ for all i; otherwise, it outputs `FALSE`.

   (e) Design a machine (*i.e.*, give the pseudocode for an algorithm) with the following function: Given 5 points $(x_1,y_1),(x_2,y_2),(x_3,y_3),(x_4,y_4),(x_5,y_5)$ with all x_i distinct, where there exists a polynomial $p(x)$ of degree at most 2 such that $p(x_i) = y_i$ for *exactly* 4 points (but we do not know which points they are), the machine outputs the index i of the point such that $p(x_i) \neq y_i$.

3. **Secret Sharing** (15 points, 5 points for each part)

   The nuclear launch "code" for the land of Hyrule is held by one person only — the princess Zelda. However, since she keeps getting kidnapped by the terroristic dark lord Ganon, she has decided to split the code across 5 old geezers.

   (a) In a stroke of brilliance, Zelda decides to try a scheme involving modular arithmetic and an integer code c where $0 \leq c \leq 2309$. In this scheme, the i-th elder knows s_i, the remainder of the code divided by the i-th prime (*i.e.*, the first elder knows c mod 2). If $(s_1,s_2,s_3,s_4,s_5) = (1,2,1,3,1)$, what is the launch code c?

   (b) Consider the standard polynomial secret sharing scheme and describe how to share c and achieve the following requirement: any 3 of the elders can be together to reconstruct the launch code, while any 2 of them cannot.

   (c) Ganon has successfully captured 2 of the 5 elders and now knows their numbers and shares of the code. Can he infer anything about the launch code in either sharing scheme? Explain your assertion. (For the time being, interpret "being able to infer anything about the code" as reducing the number of possible codes between 0 and 2309.)

4. **Error Correction Codes** (10 points, 5 points for each part)

   (a) 18 packets are transmitted on a noisy channel where at most $\frac{1}{3}$ of "all" packets will be missing (erasure error). How many packets should be sent to make sure that all packets can be recovered?

   (b) 18 packets are transmitted on a noisy channel where at most $\frac{1}{5}$ of "all" packets will be corrupted (general error). How many packets should be sent to make sure that all packets can be recovered?

5. **Countless Counting** (45 points, 3 points for each part)

   (a) How many different 13-card bridge hands are there? (A bridge hand is obtained by selecting 13 cards from a standard 52-card deck. The order of the cards in a bridge hand is irrelevant.)

   (b) How many different 13-card bridge hands are there that contain no aces?

   (c) How many different 13-card bridge hands are there that contain all four aces?

   (d) How many different 13-card bridge hands are there that contain exactly 5 spades?

   (e) Two identical decks of 52 cards are mixed together, yielding a stack of 104 cards. How many different ways are there to order this stack of 104 cards?

   (f) How many 17-bit strings are there that contain exactly 6 ones?

   (g) How many 66-bit strings are there that contain more ones than zeros?

   (h) How many different anagrams of KENTUCKY are there? (An anagram of KENTUCKY is any reordering of the letters of KENTUCKY, i.e., any string made up of the letters K, E, N, T, U, C, K and Y, in any order. The anagram does not have to be an English word.)

   (i) How many different anagrams of ALASKA are there?

   (j) How many different anagrams of CALIFORNIA are there?

   (k) How many different anagrams of MISSISSIPPI are there?

   (l) We have 8 balls, numbered 1 through 8, and 24 distinguishable bins. How many different ways are there to distribute these 8 balls among the 24 bins?

   (m) How many different ways are there to throw 8 identical balls into 24 distinguishable bins?

   (n) We throw 8 identical balls into 5 distinguishable bins. How many different ways are there to distribute these 8 balls among the 5 bins such that no bin is empty?

   (o) There are 30 students currently enrolled in a class. How many different ways are there to pair up the 30 students, so that each student is paired with one other student?

6. **Combinatorial Proof** (30 points, 10 points for each part)

   (a) n males and n females apply for the CS major at UC Berkeley. The CS department only has n seats available. How many ways can it admit students? Use the above story for a combinatorial argument to prove the following identity:

$$\binom{2n}{n} = \binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2.$$

   (b) Following Part (a), the department decides to provide two fellowships — one for a male student and the other one for a female student. Use the above story for a combinatorial argument to prove the following identity:

$$\sum_{k=1}^{n-1} k \cdot (n-k) \cdot \binom{n}{k}^2 = n^2 \cdot \binom{2n-2}{n-2}.$$

   (c) Now, come up with your own story for a combinatorial argument to prove the following identity.

$$n2^{n-1} = \binom{n}{1} + 2\binom{n}{2} + \cdots + (n-1)\binom{n}{n-1} + n\binom{n}{n}$$