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 $\mathbb{Q}$?

Answer:

(a) p and q intersect when $x = 2$; p and r do not intersect:

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

(b) p and q intersect when $x = 3$; p and r intersect when $x = 3$.

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

(c) p and q intersect when $x = 0, 2, 4$; p and r do not intersect.

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

(d) p and q intersect when $x = -2$ in both $\mathbb{R}$ and $\mathbb{Q}$. p and r intersect when $x = -\frac{3}{4}$ in both $\mathbb{R}$ and $\mathbb{Q}$. "mod 5" is most similar to $\mathbb{R}$ and $\mathbb{Q}$ as all of them have one intersection between p and q and one intersection between p and r.

(e) It is false with mod 4, and a counterexample is $(x, y) = (2, 2)$. It is false with mod 6, and a counterexample is $(x, y) = (2, 3)$. It is true with mod 5. Proof: if $(xy \equiv 0 \pmod 5)$, then $xy = 5k$ for some integer k. Since 5 is a prime (it cannot be factorized into other positive integers except 1 and itself) and 5 is a factor of xy, 5 must be a factor of x or y, which means $(x \equiv 0 \pmod 5) \vee (y \equiv 0 \pmod 5)$. Again, "mod 5" is most similar to $\mathbb{R}$ and $\mathbb{Q}$ as the statement is still true.

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 $p(x_i)\neq y_i$.

Answer:

(a) The interpolating polynomial is given by $P(x)=y_0\Delta_0(x)+y_1\Delta_1(x)+y_2\Delta_2(x)$ where

$$\Delta_0(x)=\frac{(x-1)(x-2)}{(0-1)(0-2)}=\frac{1}{2}x^2-\frac{3}{2}x+1;$$
$$\Delta_1(x)=\frac{(x-0)(x-2)}{(1-0)(1-2)}=-x^2+2x;$$
$$\Delta_2(x)=\frac{(x-0)(x-1)}{(2-0)(2-1)}=\frac{1}{2}x^2-\frac{1}{2}x.$$

Thus, we have

$$P(x)=1\left(\frac{1}{2}x^2-\frac{3}{2}x+1\right)+1\left(-x^2+2x\right)+3\left(\frac{1}{2}x^2-\frac{1}{2}x\right)=x^2-x+1.$$

(b) Yes. The polynomial in the previous question passes through the first three points. Evaluating $P(-1)=3$ verifies that it also passes through the fourth point, $(-1,3)$.

(c) No. If there existed a polynomial through those four points, then that same polynomial must necessarily pass through the first three points. However, we know that there is only one degree-2 polynomial $P(x)$, which we found in the first part, that passes through the first three points. Since $P(-1)=3\neq 0$, it does not pass through the fourth point, $(-1,0)$, and we have a contradiction.

(d) Following the intuition from the previous part: If a degree-2 polynomial passes through the four points, it must pass through the first three. Thus, we may use Lagrange interpolation to construct the unique polynomial, call it $p(x)$ through the first three points. Finally, we simply need to verify if $p(x_4)=y_4$.

Pseudocode:

```
1 Delta1(x) = [(x-x2)(x-x3)][(x1-x2)(x1-x3)]
2 Delta2(x) = [(x-x1)(x-x3)][(x2-x1)(x2-x3)]
3 Delta3(x) = [(x-x1)(x-x2)][(x3-x1)(x3-x2)]
4 p(x) = y1 * Delta1(x) + y2 * Delta2(x) + y3 * Delta3(x)
5 return P(x4) == y4
```

(e) We know that there exists a polynomial of degree at most 2 that passes through 4 of the points but not the 5th one. To find the 5th point, we can use the machine developed in part d to help us. In particular, we use the machine on all possible sets of 4 points (so we use it 5 times) to find whether or not there exists a polynomial of degree at most 2 that passes through those 4 points. Once the algorithm returns true for a set of 4 points, we know that the remaining point has the index we want to return.

Pseudocode:

```
1 if partD(x1, y1, x2, y2, x3, y3, x4, y4)
2   return 5
3 else if partD(x1, y1, x2, y2, x3, y3, x5, y5)
4   return 4
```

```
5  else if partD(x1, y1, x2, y2, x4, y4, x5, y5)
6    return 3
7  else if partD(x1, y1, x3, y3, x4, y4, x5, y5)
8    return 2
9  else if partD(x2, y2, x3, y3, x4, y4, x5, y5)
10   return 1
```

Note: This is also an approach to fix general errors, but its time complexity is very high when there are many points and many errors.

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.)

Answer:

(a) This problem reduces into a simple CRT problem, but an iterative approach also works. We know that $c = 2k_2 + 1 = 3k_3 + 2 = 5k_5 + 1 = 7k_7 + 3 = 11k_{11} + 1$ for some integers $k_2, k_3, k_5, k_7, k_{11}$.

- Consider $c = 2k_2 + 1$ and $c = 3k_3 + 2$: Since $\gcd(2,3) = 1$, there exists exactly one solution between 0 and $2 \cdot 3 - 1$. Trying all possible values (at most 2 times) of the form $c = 3k_3 + 2$ can get the solution 5, so $c = (2 \cdot 3)k_6 + 5$ for some integer k_6.
- Consider $c = 5k_5 + 1$ and $c = 6k_6 + 5$: Since $\gcd(5,6) = 1$, there exists exactly one solution between 0 and $5 \cdot 6 - 1$. Trying all possible values (at most 5 times) of the form $c = 6k_6 + 5$ can get the solution 11, so $c = (5 \cdot 6)k_{30} + 11$ for some integer k_{30}.
- Consider $c = 7k_7 + 3$ and $c = 30k_{30} + 11$: Since $\gcd(7,30) = 1$, there exists exactly one solution between 0 and $7 \cdot 30 - 1$. Trying all possible values (at most 7 times) of the form $c = 30k_{30} + 11$ can get the solution 101, so $c = (7 \cdot 30)k_{210} + 101$ for some integer k_{210}.
- Consider $c = 11k_{11} + 1$ and $c = 210k_{210} + 101$: Since $\gcd(11,210) = 1$, there exists exactly one solution between 0 and $11 \cdot 210 - 1$. Trying all possible values (at most 11 times) of the form $c = 210k_{210} + 101$ can get the solution 2201, so $c = (11 \cdot 210)k_{2310} + 2201$ for some integer k_{2310}.

Since $c \in [0, 2309]$, we know that $c = 2201$.

(b) Find a prime q larger than 2309, work over $GF(q)$, and pick any polynomial of degree 2 that has $P(0) = 2201$. One such solution is to use $q = 2311$ and $P(x) = 1000x^2 + 2201$, get

$(1,890),(2,1579),(3,1957),(4,2024),(5,1780)$, accordingly. Then, give one point to each elder. Any 3 of the elders can be together to reconstruct $P(x)$ and $P(0)$, while any 2 of them cannot.

(c) If he has captured 2 of the 5 elders, he knows nothing in the polynomial scheme in Part (b). This is because, for every value of three points, we can define a different polynomial for every possible $P(0)$. However, in the scheme in Part (a), Ganon can solve a simplified CRT problem (as the intermediate steps in Part (a)) and obtain information about c mod n where n is the product of the captured primes. For example, if he has captured primes p_1, p_2, then he can determine c mod p_1p_2. If he has captured even a single prime p, he can reduce $\frac{p-1}{p}$ of his search space.

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?

Answer:

(a) We observe that the worst case is when $1/3$ packets are missing. Assume m is the number of all packets, m must satisfy

$$m - \frac{1}{3}m \geq 18,$$

which means that the number of all packets minus the number of missing packets must be at least 18. Solving the inequality can get $m \geq 27$.

Note: Students can get bonus points by trying to minimize the number of packets and answering 26. This is true because the more precise inequality is

$$m - \left\lfloor \frac{1}{3}m \right\rfloor \geq 18.$$

(b) We observe that the worst case is when $1/5$ packets are corrupted. Assume m is the number of all packets, m must satisfy

$$\frac{4}{5}m - \frac{1}{5}m \geq 18,$$

which means that the number of correct packets minus the number of corrupted packets must be at least 18. Solving the inequality can get $m \geq 30$.

Note: Students can get bonus points by trying to minimize the number of packets and answering 28. This is true because the more precise inequality is

$$\left\lceil \frac{4}{5}m \right\rceil - \left\lfloor \frac{1}{5}m \right\rfloor \geq 18.$$

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?

Answer:

(a) This is sampling without replacement and order does not matter. $\binom{52}{13}$.

(b) There are 48 cards excluding aces. $\binom{48}{13}$.

(c) The four aces are fixed, so there are 9 other cards in your hand. $\binom{48}{9}$.

(d) There are $\binom{13}{5}$ ways to get 5 spades, and $\binom{39}{8}$ ways to get the remaining 8 cards. $\binom{13}{5} \cdot \binom{39}{8}$.

(e) There are 104! permutations of the whole deck, and each of the 52 cards has two permutations (since there are two identical cards in this double-deck). Therefore, there are $104!/2^{52}$ ways to order the deck.

(f) A bitstring contains ones and zeros. Selecting the position of the 6 ones is the important part of this problem. $\binom{17}{6}$.

(g) One approach is to consider all strings with 34 or more ones, so there are $\sum_{i=34}^{i=66} \binom{66}{i}$ bitstrings. Another approach is to consider that all bitstrings have either more ones, more zeros, or an equal amount of each, and the number with more ones is equal to the number with more zeros. The number of bitstrings is 2^{66}, excluding bitstrings with 33 ones is $2^{66} - \binom{66}{33}$, and dividing by 2 yields $\frac{2^{66}-\binom{66}{33}}{2}$.

(h) There are 2 K's and 8 letters, so there are $\frac{8!}{2!}$ different anagrams.

(i) There are 3 A's and 6 letters, so $\frac{6!}{3!}$ different anagrams.

(j) There are 2 I's and 2 A's and 10 letters, so $\frac{10!}{2!2!}$ different anagrams.

(k) There are 4 I's, 4 S's, 2 P's, and 11 letters, so $\frac{11!}{4!4!2!}$ different anagrams.

(l) The balls are distinct. Each ball can go into any of the 24 bins, so there are 24^8 different distributions.

(m) The balls are indistinguishable. There are $\binom{24+8-1}{8} = \binom{31}{8}$ different ways.

(n) Since no bin is empty, there is at least one ball in each bin, and three balls remain after that. Therefore there are $\binom{5+3-1}{3} = \binom{7}{3}$ ways to distribute the balls as described.

(o) There are many ways to solve this problem. Here are three.

- Approach 1: This problem can be thought of as throwing 30 distinct balls (students) into 15 indistinguishable bins (pairs) such that each bin has 2 balls. There are 15! permutations of bins and $\frac{30!}{2^{15}}$ ways to throw the balls into bins as described, so there are $\frac{30!}{2^{15}15!}$ different pairings total.
- Approach 2: Another way to think of the problem is by randomly selecting 15 students to send to Mars, then matching each student on Earth with a student on Mars. There are $\binom{30}{15}$ ways to select students to send to Mars. There are 15! ways to pair the students on Earth each with a student on Mars. However, this counts matching Alice on Mars with Bob on Earth as different from matching Bob on Mars with Alice on Earth. For each of the 15 students, we counted twice, so we need to divide by 2^{15}. Our final answer is $\binom{30}{15}\frac{15!}{2^{15}}$, which is indeed equal to $\frac{30!}{2^{15}15!}$.
- Approach 3: One more way to think of this problem is to order the students arbitrarily (say by height). Randomly match the tallest student with one of the remaining 29 students. Then randomly match the tallest remaining student with one of the remaining 27 students. Continue this until all students are matched. The final answer is $29 \cdot 27 \cdot 25 \cdot \ldots \cdot 3 \cdot 1$. You can check that this is equal to the other answers.