CS 70 Discrete Mathematics and Probability Theory
Spring 2016 Rao and Walrand HW 5

Due Thursday 18th at 10PM

1. **Proof practice**

   The purpose of this problem is to practice formally proving a statement, when you intuitivelly "know" why it's true.

   Suppose that there are n chickens in a farmyard. Chickens are rather aggressive birds that tend to establish dominance in relationships by pecking. (Hence the term "pecking order".) In particular, for each pair of distinct chickens, either the first pecks the second or the second pecks the first, but not both. We say that chicken u virtually pecks chicken v if either:

   - Chicken u directly pecks chicken v, or
   - Chicken u pecks some other chicken w who in turn pecks chicken v.

   A chicken that virtually pecks every other chicken is called a *king chicken*.

   We can model this situation with a tournament digraph. The vertices are chickens, and an edge $u \to v$ indicates that chicken u pecks chicken v. Notice that there could be multiple kings.

   Theorem 1. *The chicken with the largest outdegree in an n-chicken tournament is a king.*

   Intuitively the theorem is true because if the chicken with the largest outdegree was not a king then there would be a chicken that pecks everyone that the fake king pecks, as well as the fake king, i.e. have an even larger outdegree.

   Turn this intuition into a formal proof.

   Answer:

   By contradiction, let u^* be the chicken with the largest outdegree, and assume it is not a king. Let $X = \{v|(u^*,v) \in E\}$ be the set of chicken that are pecked by u^*, and $Y = \{v|(x,v) \in E, x \in X\}$ the set of chicken that are pecked by chickens in X. The outdegree of u^* is equal to $|X|$.

   Let z be a chicken such that $z \notin X \cup Y$. This implies that $(v,z) \notin E$, for all $v \in X \cup \{u^*\}$. But, by the tournament property, this implies that $(z,v) \in E$, for all $v \in X \cup \{u^*\}$. Therefore the degree of z is equal to $|X|+1 > |X|$, a contradiction, since u^* has the highest outdegree.

2. **What's in a googolplex?**

   A "googolplex", the namesake of Google's "Googleplex" headquarters, is the number written as 1 followed by 10^{100} zeroes. That is, it's $10^{10^{100}}$. For a positive integer n, we define "n factorial" (written $n!$) as the product of all positive integers from 1 to n, i.e. $n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$. As you might imagine, $10^{10^{100}}!$, googleplex factorial, is a Very Large Number. Let:

   $$\begin{aligned} m \;=\; & 5185925986735423542444467237838883862213453463463453456 2 \\ & 4343453463442098164524359134591810007513111459435723459 1 \\ & 1023509823745752342345759111744904220352511745677798903 1. \end{aligned}$$

Note that that's a single 168-digit number (it just doesn't fit onto one line). Calculate what $10^{10^{100}}!$ is congruent to, modulo m. That is, find the value of:

$$10^{10^{100}}! \mod m$$

Show all your work. Hint: if your answer takes more than 5-10 lines of text, you are probably doing it wrong.

Answer: The key observation is that, since m has 168 digits, $m < 10^{169} < 10^{10^{100}}$. Thus m must be one of the factors comprising googleplex factorial by definition, which means that googleplex factorial must be divisible by m and hence congruent to 0 modulo m. If you want to be exceedingly formal about it:

$$\begin{aligned}
10^{10^{100}}! \mod m &= \left(\prod_{i=1}^{10^{10^{100}}} i\right) \mod m \\
&= \left(\prod_{i=1}^{10^{10^{100}}} (i \mod m)\right) \mod m \\
&= \left(\prod_{i=1}^{m-1} (i \mod m)\right) \cdot (m \mod m) \cdot \left(\prod_{i=m+1}^{10^{10^{100}}} (i \mod m)\right) \mod m \\
&= \left(\prod_{i=1}^{m-1} (i \mod m)\right) \cdot 0 \cdot \left(\prod_{i=m+1}^{10^{10^{100}}} (i \mod m)\right) \mod m \\
&= 0
\end{aligned}$$

3. **(Polynomial Interpolations)**

   (a) Consider the set of four points $\{(0,1),(1,-2),(3,4),(4,0)\}$, construct the unique degree-3 polynomial (over the reals) that passes through these four points by writing down and solving a system of linear equations.

   Answer: Suppose the unique degree 3 polynomial passing through the four given points is

   $$p(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3$$

   The coefficients of $p(x)$ satisfy the following linear equations:

   $$p(0) = 1 \Rightarrow a_0 = 1 \tag{1}$$
   $$p(1) = -2 \Rightarrow a_0 + a_1 + a_2 + a_3 = -2 \tag{2}$$
   $$p(3) = 4 \Rightarrow a_0 + 3a_1 + 9a_2 + 27a_3 = 4 \tag{3}$$
   $$p(4) = 0 \Rightarrow a_0 + 4a_1 + 16a_2 + 64a_3 = 0 \tag{4}$$

   Substituting $a_0 = 1$ and subtracting (i) 3 times equation (2) from equation (3) and (ii) 4 times equation (2) from equation (4), we obtain the following simultaneous equations:

   $$6a_2 + 24a_3 = 12$$
   $$12a_2 + 60a_3 = 11$$

Solving for a_2 and a_3, we obtain $a_2 = 76/12$ and $a_3 = -13/12$. Substituting in equation (2) we obtain $a_1 = -99/12$. Hence

$$p(x) = (12 - 99x + 76x^2 - 13x^3)/12$$

is the unique degree 3 polynomial passing through the given points.

(b) Use Lagrange interpolation to find a polynomial $p(x)$ of degree at most 2 that passes through the points $(1,2)$, $(2,3)$, and $(3,5)$, working in $GF(7)$. In other words, we want $p(x)$ to satisfy $p(1) \equiv 2 \pmod 7$, $p(2) \equiv 3 \pmod 7$, and $p(3) \equiv 5 \pmod 7$. Show your work clearly and use the same notations as in Lecture Note 8.

Answer: First we would find the three $\Delta_i(x)$ polynomials.

$$\Delta_1(x) \equiv \frac{(x-2)(x-3)}{(1-2)(1-3)} \equiv \frac{(x-2)(x-3)}{2} \equiv 4(x-2)(x-3) \equiv 4x^2 + x + 3 \pmod 7$$
$$\Delta_2(x) \equiv \frac{(x-1)(x-3)}{(2-1)(2-3)} \equiv \frac{(x-1)(x-3)}{-1} \equiv -(x-1)(x-3) \equiv 6x^2 + 4x + 4 \pmod 7$$
$$\Delta_3(x) \equiv \frac{(x-1)(x-2)}{(3-1)(3-2)} \equiv \frac{(x-1)(x-2)}{2} \equiv 4(x-1)(x-2) \equiv 4x^2 + 2x + 1 \pmod 7$$

Next we compute $p(x)$:

$$\begin{aligned} p(x) &\equiv 2\Delta_1(x) + 3\Delta_2(x) + 5\Delta_3(x) \pmod 7 \\ &\equiv 2(4x^2 + x + 3) + 3(6x^2 + 4x + 4) + 5(4x^2 + 2x + 1) \pmod 7 \\ &\equiv x^2 + 2x + 6 + 4x^2 + 5x + 5 + 6x^2 + 3x + 5 \pmod 7 \\ &\equiv 4x^2 + 3x + 2 \pmod 7 \end{aligned}$$

4. **Secret Sharing**

Suppose we wish to share a secret among five people, and we decide to work modulo 7. We construct a degree-two polynomial $q(x) = ax^2 + bx + s$ by picking the coefficients a and b at random (mod 7); the constant term is the secret s (also a number mod 7). We give shares $q(1), \ldots, q(5)$ to each of the five people (all operations being done mod 7). Now suppose that three of the people get together and share the information that $q(1) = 5$, $q(2) = 2$, and $q(4) = 2$. Use Lagrange interpolation to find the polynomial q and the secret s. Show all your work.

Answer: For convenience, we will first list the inverse pairs modulo 7: $(1,1), (2,4), (3,5), (6,6)$. Now, to find a polynomial q such that $q(1) = 5$, $q(2) = 2$, and $q(4) = 2$, we must compute

$$q(x) = 5\Delta_1(x) + 2\Delta_2(x) + 2\Delta_4(x),$$

where each Δ_i is computed as follows:

$$\begin{aligned} \Delta_1 &= \frac{(x-2)(x-4)}{(1-2)(1-4)} = \frac{x^2 - 6x + 8}{(-1)(-3)} = 5(x^2 + x + 1) = 5x^2 + 5x + 5 \\ \Delta_2 &= \frac{(x-1)(x-4)}{(2-1)(2-4)} = \frac{x^2 - 5x + 4}{(1)(-2)} = 3(x^2 + 2x + 4) = 3x^2 + 6x + 5 \\ \Delta_4 &= \frac{(x-1)(x-2)}{(4-1)(4-2)} = \frac{x^2 - 3x + 2}{(3)(2)} = 6(x^2 + 4x + 2) = 6x^2 + 3x + 5 \end{aligned}$$

Substituting, we now have

$$\begin{aligned} q(x) &= 5(5x^2+5x+5)+2(3x^2+6x+5)+2(6x^2+3x+5) \\ &= (4x^2+4x+4)+(6x^2+5x+3)+(5x^2+6x+3) \\ &= x^2+x+3 \end{aligned}$$

5. **Properties of $GF(p)$**

   (a) Show that, if $p(x)$ and $q(x)$ are polynomials over the reals (or complex, or rationals) and $p(x) \cdot q(x) = 0$ for all x, then either $p(x) = 0$ for all x or $q(x) = 0$ for all x or both.

   Answer: We will show the contrapositive. Suppose that $p(x)$ and $q(x)$ are both non-zero polynomials of degree d_p and d_q respectively. Then $p(x) = 0$ for at most d_p values of x and $q(x) = 0$ for at most d_q values of x. Since there are an infinite number of values for x (because we are using complex, real, or rational numbers) we can always find an x, call it $x_{notzero!}$, for which $p(x_{notzero!}) \neq 0$ and $q(x_{notzero!}) \neq 0$. This gives us $p(x_{notzero!}) \cdot q(x_{notzero}) \neq 0$, so pq is non-zero.

   (b) Show that the claim in part (a) is false for finite fields $GF(p)$.

   Answer: In $GF(p)$, $x^{p-1}-1$ and x are both non zero polynomials, but when p is prime, their product $(x^p - x)$ is zero for all x by Fermat's little Theorem.
   Examples for a specific p are also acceptable. For example for $GF(2)$, $p(x) = x$ and $q(x) = x+1$ work.