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.

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:

   $$\begin{aligned} m \;=\; & 518592598673542354244446723783888386221345346346345345624343453463442098164524359134591810007513111459435723459110235098237457523423457591117449042203525117456777989031. \end{aligned}$$

   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.

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.

   (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.

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.

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.

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