CSE 311: Foundations of Computing (Spring, 2015)

Homework 4 Out: Friday, 24-Apr. Due: Friday, 1-May, **before class (1 pm)** on **Gradescope**

Additional directions: You should write down carefully argued solutions to the following problems. Your first goal is to be complete and correct. A secondary goal is to keep your answers simple and succinct. The idea is that your solution should be easy to understand for someone who has just seen the problem for the first time. (Re-read your answers with this standard in mind!) You may use any results proved in lecture (without proof). Anything else must be argued rigorously. For this homework, you can write your proofs in English.

1. So much **fun**ction (10 points)

Each of the following functions maps the non-negative integers $\mathbb{N}$ to the non-negative integers $\mathbb{N}$. For each one, indicate the following: (i) its range, (ii) whether the function is one-to-one, (iii), whether the function is onto. Briefly justify your answers.

(a) $f(n) = 3^n$

(b) $f(n) = n + 1$ if n is even and $f(n) = \frac{3n+1}{2}$ if n is odd.

(c) $f(n) = n^2 - 2n + 1$

(d) $f(n)$ = the smallest integer k such that $3^k \geq n + 1$.

(e) $f(n)$ = # of distinct prime factors dividing $n + 1$.

2. You got sets appeal (10 points)

Prove or disprove: For all sets X, Y, Z, if $X \cup Z = Y \cup Z$ and $X \cap Z = Y \cap Z$, then $X = Y$.

3. Powerful power (10 points)

Prove that $A = B$ if and only if $\mathcal{P}\big(\mathcal{P}(A)\big) = \mathcal{P}(\mathcal{P}(B))$.

[Hint: Make things easy on yourself by proving a less powerful statement first.]

4. A disturbing poem left in my office hours (12 points)

that
boy who
sits near the front
had better not turn around. cheese wheel.

(a) Prove that if n is an integer, then n^2 is congruent modulo 7 to the number of words in one of the lines of the disturbing poem.

(b) Prove that if $p > 3$ is prime, then $p \bmod 6 \in \{1,5\}$.

5. Modular numerology (10 points)

Let a, b be integers and c, m positive integers. Prove that if $ac \equiv bc \pmod{cm}$, then $a \equiv b \pmod{m}$.

6. Palindromes (15 points)

The numbers 214412 and 278872 read the same forward and backward when written in decimal. Prove that every such number with an even number of digits is divisible by 11. [Hint: Recall our proof from lecture that a number is divisible by 3 if and only if the sum of its digits is.]

7. **Extra credit**: Error-correcting codes

When a message is encoded on or transmitted over a possibly noisy medium, we would like to have some way to quickly recover the entire message even if parts of it have been corrupted. This leads to the study of **error-correcting codes**. Such codes are the reason that a DVD or Bluray can be scratched up pretty badly and still play perfectly. They're also used for satellite communication, and QR codes like

More formally, we would like to encode n-bit strings by m-bit strings. Such an encoding can be specified as a map $C : \{0,1\}^n \to \{0,1\}^m$. We want to have the property that for every message M, even if many bits of the encoded message $C(M)$ are corrupted, we can still recover M. The catch here is that we have no idea where the errors will occur, and no matter what we should be able to do the recovery. So the original message has to be "smeared" through the entire encoding $C(M)$.

A good code should be able to recover from many errors (e.g., 10% of bits corrupted) and have m/n as small as possible (so that we don't expand the length of the message by too much---we don't want to give up too much capacity in order to obtain error correction). We won't touch on it here, but it's also important that we can do encoding and decoding (of the noisy encoded message) very fast. For instance, your DVD player does this in real time as it plays the movie.

The encoding. Let p be a prime number, and let $\mathbb{F}_p = \{0,1,2,\dots,p-1\}$ be the finite field of size p. Multiplication and addition in $\mathbb{F}_p$ are done modulo p. This is called a **field** because, as we will see (or have seen) in lecture, it is closed under addition and multiplication, every element has an additive inverse, and every element except for 0 has a multiplicative inverse (for every $a \in \mathbb{F}_p$ with $a \neq 0$, there is an element $x \in \mathbb{F}_p$ such that $ax \equiv 1 \pmod{p}$).

Fix natural numbers $t > k \geq 1$. Fix a subset $S \subseteq \mathbb{F}_p$ with $S = \{x_1, x_2, \dots, x_t\}$ for some $t \leq p$.

We will think of a message as a sequence $M = (m_0, m_1, \dots, m_{k-1})$ with each $m_i \in \mathbb{F}_p$. We interpret the message M as a **polynomial** in the following way:

$$q_M(x) = m_0 + m_1 x + m_2 x^2 + \cdots + m_{k-1} x^{k-1}$$

We define the encoding of the message M by evaluating this polynomial at the points of S:

$$C(M) = \big(q_M(x_1), q_M(x_2), \dots, q_M(x_t)\big).$$

(a) How many its do we need to represent the message M? How many bits to represent the encoded message $C(M)$? What is the blow-up in size of $C(M)$ over M?

Your goal now will be to prove that this is a good error-correcting code. The encoding $C(M)$ consists of t numbers mod p. You will show that if at most $\frac{t-k+1}{2}$ of these numbers are corrupted, we can still recover the original message M.

(b) Let $q(x) = c_d x^d + c_{d-1} x^{d-1} + \cdots + c_1 x + c_0$ be a polynomial with coefficients $c_i \in \mathbb{F}_p$. Prove that $q(x)$ has at most d roots, i.e. there are at most d distinct numbers $a_1, \dots, a_d \in \mathbb{F}_p$ such that $q(a_i) = 0$.

The basic idea is to suppose that $q(a_1) = 0$ and then try to write $q(x) = (x - a_1)\, r(x)$ where $\deg(r) \leq d - 1$. You will then argue that $r(a_i) = 0$ for $i > 1$ and keep going.

To do this, try to find a way of writing $q(x) = c_d (x - a_1)^d + s(x)$ where $\deg(s) \leq d - 1$.

(c) Consider now a message $M = (m_0, m_1, \dots, m_{k-1})$ and its encoding $C(M) = \big(q_M(x_1), q_M(x_2), \dots, q_M(x_t)\big)$. Suppose the encoding is corrupted, so that we receive the values $\tilde{C}(M) = (z_1, z_2, \dots, z_t)$ where $z_i = q_M(x_i)$ except possibly for $\left\lfloor \frac{t-k+1}{2} \right\rfloor$ indices where z_i is corrupted. Prove that under this assumption, there is a unique message M corresponding to $\tilde{C}(M)$.

In other words, prove that if at most $t - k + 1$ values are corrupted, then no other message $M' \neq M$ can have $\tilde{C}(M) = \tilde{C}(M')$. [Hint: Use part (b) and consider the polynomial $q_M - q_{M'}$.]

8. Extra credit: Pokémons on a plane, episode 2.

Consider the predicates $\mathrm{Pokemon}(x), \mathrm{Celebrity}(x), \mathrm{Jet}(x), \mathrm{WearsPants}(x)$, $\mathrm{Flies}(x, y)$ which denote, respectively, that x is a Pokémon, celebrity, or jet, that x wears pants, and that person x flies on jet y. We also use $\mathrm{Alive}(x)$ to denote that x is alive. (For the purposes of this problem, celebrities are alive, even if they're a little dead inside. Pokémon are definitely alive.) $\mathcal{T}$ is Taylor's jet and is $\mathcal{B}$ Bieber's jet. The domain of discourse is the set of all alive things and all flying things.

Suppose the following are true:

(i) $\forall x \left(\mathrm{Flies}(x, \boldsymbol{\mathcal{T}}) \leftrightarrow \left(\mathrm{Pokemon}(x) \wedge \mathrm{WearsPants}(x)\right)\right)$

(ii) $\forall x \left(\mathrm{Flies}(x, \boldsymbol{\mathcal{B}}) \leftrightarrow \left(\mathrm{Celebrity}(x) \wedge \mathrm{WearsPants}(x)\right)\right)$

(iii) $\forall j \left(\mathrm{Jet}(j) \rightarrow \exists x\left(\mathrm{Alive}(x) \wedge \neg \mathrm{Flies}(x, j)\right)\right)$

(iv) $\forall j \left(\mathrm{Jet}(j) \rightarrow \exists h \left(\mathrm{Jet}(h) \wedge \forall x \left(\mathrm{Alive}(x) \rightarrow \left(\mathrm{Flies}(x, h) \leftrightarrow \neg \mathrm{Flies}(x, j)\right)\right)\right)\right)$

Explain precisely why there is at least one Pokémon who is not allowed to fly on Taylor's jet.

[Those few students who figured this out in the last round get double points---no need to (not) solve it again.]