CS 70 Discrete Mathematics and Probability Theory
Spring 2019 Course Notes **HW 6**

Due: Friday, March 8th, 10pm

Sundry

Before you start your homework, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Error-Detecting Codes

Suppose Alice wants to transmit a message of n symbols, so that Bob is able to *detect* rather than *correct* any errors that have occured on the way. That is, Alice wants to find an encoding so that Bob, upon receiving the code, is able to either

(I) tell that there are no errors and decode the message, or

(II) realize that the transmitted code contains at least one error, and throw away the message.

Assuming that we are guaranteed a maximum of k errors, how should Alice extend her message (i.e. by how many symbols should she extend the message, and how should she choose these symbols)? You may assume that we work in GF(p) for very large prime p. Show that your scheme works, and that adding any lesser number of symbols is not good enough.

2 Berlekamp-Welch Algorithm with Fewer Errors

In class we derived how the Berlekamp-Welch algorithm can be used to correct k general errors, given $n+2k$ points transmitted. In real life, it is usually difficult to determine the number of errors that will occur. What if we have less than k errors? This is a follow up to the exercise posed in the notes.

Suppose Alice wants to send 1 message to Bob and wants to guard against 1 general error. She decides to encode the message with $P(x) = 4$ (on GF(7)) such that $P(0) = 4$ is the message she want to send. She then sends $P(0), P(1), P(2) = (4,4,4)$ to Bob.

(a) Suppose Bob receives the message $(4,5,4)$. Without performing Gaussian elimination explicitly, find $E(x)$ and $Q(x)$.

(b) Now, suppose there were no general errors and Bob receives the original message $(4,4,4)$. Show that the $Q(x),E(x)$ that you found in part (a) still satisfies $Q(i)=r_iE(i)$ for all $i=0,1,2$.

(c) Verify that $E(x)=x$, $Q(x)=4x$ is another possible set of polynomials that satisfies $Q(i)=r_iE(i)$ for all $i=0,1,2$.

(d) Suppose you're actually trying to decode the received message $(4,4,4)$. Based on what you showed in the previous two parts, what will happen during row reduction when you try to solve for the unknowns?

(e) Prove that no matter what the solution of $Q(x)$ and $E(x)$ are though, the recovered $P(x)$ will always be the same.

3 Counting Cartesian Products

For two sets A and B, define the cartesian product as $A\times B=\{(a,b):a\in A,b\in B\}$.

(a) Given two countable sets A and B, prove that $A\times B$ is countable.

(b) Given a finite number of countable sets $A_1,A_2,\ldots,A_n$, prove that

$$A_1\times A_2\times\cdots\times A_n$$

is countable.

(c) Consider an infinite number of countable sets: $B_1,B_2,\ldots$. Under what condition(s) is $B_1\times B_2\times\cdots$ countable? Prove that if this condition is violated, $B_1\times B_2\times\cdots$ is uncountable.

4 Counting Tools

Are the following sets countable or uncountable? Please prove your claims.

(a) $\bigcup_{i\in A}B_i$, where A,B_i are all countable.

(b) The set of all functions f from $\mathbb{N}$ to $\mathbb{N}$ such that f is non-decreasing. That is, $f(x)\leq f(y)$ whenever $x\leq y$.

(c) The set of all functions f from $\mathbb{N}$ to $\mathbb{N}$ such that f is non-increasing. That is, $f(x)\geq f(y)$ whenever $x\leq y$.

(d) The set of all bijective functions from $\mathbb{N}$ to $\mathbb{N}$.

5 Fixed Points

Consider the problem of determining if a function F has any fixed points; that is, we want to know if there is any input x such that $F(x)$ outputs x. Prove that this problem is undecidable.

6 Kolmogorov Complexity

Compression of a bit string x of length n involves creating a program shorter than n bits that returns x. The Kolmogorov complexity of a string $K(x)$ is the length of shortest program that returns x (i.e. the length of a maximally compressed version of x).

(a) Explain why "the smallest positive integer not definable in under 100 characters" is paradoxical.

(b) Prove that for any length n, there must be at least one bit string that cannot be compressed.

(c) Imagine you had the program K, which outputs the Kolmogorov complexity of string. Design a program P that when given integer n outputs the bit string of length n with the highest Kolmogorov complexity. If there are multiple strings with the highest complexity, output the lexicographically first (i.e. the one that would come first in a dictionary).

(d) Suppose the program P you just wrote can be written in m bits. Show that P and by extension, K, cannot exist, for a sufficiently large input n.