CS 1511 Homework 26

Mathew Varughese, Justin Kramer, Zach Smith

Mon, Apr 15

53. Each bit has either a probabiltiy of 1 or 0. There is not a way to tell how the message was formed, so a machine can be made that outputs a coin flip that has the same answer.

54. If P=NP then any problem that can be solved by a nondeterministic polynomial TM can be solved by a deterministic polynomial TM. A one way function can be inverted if one tests all possible values x to check if $f(x) = y$ where y is the output that is trying to be reversed. This is a NP problem, because the certificate would be x. So, if P=NP, then this could be solved in polynomial time, and any one-way function would be reversible in polynomial time, thus contradicting the defintion of a one way function.

55. $f(x)$ is a one way permutation. A one way permutation is a function that maps n bits to n bits and for every BPP machine C, C(f(x)) = x has a very small probability.

Thus, f(f(x)) will have the same property. Since x is not discoverable from f(x), f(f(x)) also has the same property. It is a one way function.

This idea can be repeated for all f^k functions. Since k is polynomial,