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. The distributions of $E_{U_n}(x)$ and $E_{U_n}(x')$ can not be identical if $n < m$ because there must be an n that maps to two m's, which means that if you have one of the n's then there's a greater possibility of these two answers for your initial message, which destroys the possibility that you have the same distribution for all messages once run through the function E.

You need to have at least one n for each m so that for each key n, it could map to any m so that all distributions of E are identical.

56. Assume by contradiction that f^k is not a one-way permutation. Now say we have a polynomial time algorithm A that we apply f^k to in order to get a probability for (A(y) = y) that is greater than some negligible amount for all n.

We can then convert our probability with this composition into $f(f^{k-1}(A(y) = y)$.

We know that $f^{k-1}A(y)$ can be computed in polynomial time. So we can compute A(y) and then apply our permutation f (k - 1) times, which will takes n^c (a poly amount of times of f which is poly-time). This now contradicts that f is a one-way permutation.