Assignment 5

COMP 531 Winter 2016

Due April 18th

1. Let H be a universal family of hash functions from n bits to m bits. Let $U \subset \{0,1\}^n$ be a set of elements to be hashed.

   a) Let $a = |U|/2^m$. Prove that

   $$(a - \frac{a}{2}) \leq Pr_{h,t}[\exists x \in U \text{ such that } h(x) = t] \leq a$$

   b) Suppose $2^{m-2} \leq |U| \leq 2^{m-1}$. Call an element x of U isolated by h if for all $y \in U, y \neq x$, $h(x) \neq h(y)$. Show that the expected number of elements isolated by a random $h \in H$ is at least $|U|/2$. Show that

   $$Pr_{h,t}[\exists! x \in U \text{ such that } h(x) = t] \geq \frac{1}{8}$$

2. Prove that if SAT $\in$ **BPP**, then SAT $\in$ **RP**. Conclude that if **NP** $\subseteq$ **BPP**, then **NP** = **RP**.

3. A graph $G = (V, E)$ is called an (n, d, c)-expander if the graph has n vertices with maximum degree d and satisfies the following property: for every subset W of vertices, if $|W| \leq n/2$, then $|N(W) \cup W| \geq (1 + c)|W|$. Here, $N(W)$ denotes the neighborhood of W, i.e. all the vertices adjacent to a vertex in W. In onther words, W "expands" when we take its neighbors in the graph. It's not at all obvious that such graphs exist, but the exercise below outlines such a proof.

   Consider n to be even. We build a random graph G_n by picking d matchings independently and uniformly at random. A convenient way to think about picking a matching is as follows. Choose an arbitrary unmatched vertex, and choose another unmatched vertex at random from the remaining ones. Match them, and repeat the process until all vertices have been exhausted. Now consider all pairs (W, Q) such that if $N(W) \cup W \subseteq Q$, then W doesn't expand. For any such (W, Q) pair, upper-bound the probability that $N(W) \cup W \subseteq Q$. Sum this up over all pairs and show that for each c, there exists a d for which this sum is less than 1. Conclude that expanders must therefore exist.

4. You may be wondering why you proved that expanders exist. We can use expanders to amplify the correctness of **RP** algorithms. Let G be a $(2^n, 5, (2-\sqrt{3})/4)$-expander. Use n bits of randomness to pick a random starting node in G. For $\delta = O(logn)$, find all the nodes $y_1, \ldots, y_k$ that are withing distance δ of your starting node. Run the RP algorithm k times using that y's instead of random strings. Prove that this method will lower the probability of error to $1/n^c$ for some constant c

5. Show that the problem GI is downward self reducible. That is, prove that given two graphs G_1, G_2 on n vertices and access to a subroutine P that solves the GI problem on graphs with up to $n-1$ vertices, we can decide whether or not G_1 and G_2 are isomorphic in polynomial time.