Sreeram Danda
CS577 Homework #3
Problem #5

#5

Let $G = (V, E)$ be a graph where V are the vertices and E is the edge connecting vertices. Let $Z_p = \{0, 1, 2, ..., p - 1\}$ and $Z^*_p = \{1, 2, ..., p - 1\}$ where p is a prime > $|V|$. Let $U = Z_p$. For every pair (a,b) where $a \in Z^*_p$ and $b \in Z_p$, let $h_{ab}(x) = (ax + b) mod\ 2$ be a hash function from U to {0,1}. Set $H = \{h_{ab}:\ a \in Z^*_p$ and $b \in Z_p\}$, so *H* contains p(p-1) functions. For every vertex *V* in *G*, compute h_{ab} . Each value will be either 0 or 1, so we can assign that vertex to group V_0 or V_1 based on the value of h(v). We know that *H* is a universal family of hash functions, so $\{h_{ab}(x)\}_{a,b\in Z_p,\, a\neq 0}$ is also a universal family of hash functions. We can then denote a cut from the above algorithm as $C = \{(v_1, v_2) | h_{ab}(v_1) \neq h_{ab}(v_2)\}$. Since we established that we are using a universal family of hash functions, the probability $h_{ab}(v_1) \neq h_{ab}(v_2)$ is equal to ½. Since there are a polynomial amount of pairs of *a* and *b* values that can be chosen we can examine all the possible cuts obtained from the algorithm in polynomial time. Then look at all the cuts and choose the one that is at least 50% of the maximum possible. We know from analysis of the "monkey method" that the expected cut size E[C] = |G|/2. Since G can be represented as a polynomial using the universal hash family, at least one cut must be $|G|^k/2$ where k is some constant.