CSC 323 Algorithm Design and Analysis
Spring 2015

Instructor: Dr. Natarajan Meghanathan

Project 6
Theorem Proving Project: Bloom Filters, Breadth First Search and Asymptotic Complexity

Submission:
(1) Hardcopy report of your proofs for each task
(2) Desktop recorded videos of the explanation of the proofs, uploaded through Google Drive to my email address: natarajan.meghanathan@jsums.edu
Due: April 9, 2015: 1 PM **Max. Points: 100**

In this project, you will prove things as required below in each of the tasks and record your proof in a video (desktop recording). You will submit a hardcopy report of your proofs for each task and submit the video through Google Drive. Try to submit just a single video that includes a recording of your proof for all the three tasks (instead of three separate videos).

Task 1 (40 points): Bloom filters are considered an application of hash tables. Bloom filters are used for proactive password cracking - to identify whether a password entered by a user at the time of registration is vulnerable for cracking or not. To do so, the Bloom filter maintains the hash values for a potentially vulnerable list of passwords (commonly used passwords, words from dictionary, etc) and if the hash value of the user entered password matches to those in the Bloom filter, the user password is not accepted as part of the registration process and the user is forced to choose a password whose hash value does not match to the one in the Bloom filter.

For the purpose of this project, you could envision a Bloom filter that calculates the hash value for a word as the sum of the ascii values of the characters in the word divided by a prime number; the size of the Bloom filter (hash table) is the magnitude of the divisor prime number. You can assume either a closed or open hash table.

A false positive scenario is one wherein the user entered password is not vulnerable; but a Bloom filter flags the password as vulnerable. A false negative scenario is one wherein the user entered password is vulnerable; but a Bloom filter does not flag the password as vulnerable.

Given the above description of Bloom filters, prove that the Bloom filters cannot have a false negative scenario, but could have a false positive scenario. You could show your proof with examples and record a video.

Task 2 (30 points): Prove that when Breadth First Search (BFS) is conducted on a graph starting from a particular vertex *s*, we are guaranteed to find the minimum hop path (paths with the minimum number of intermediate edges) from *s* to every other vertex in the graph.

Task 3 (30 points): In Module 1, we proved in class that if $t_1(n) \in O(g_1(n))$ and $t_2(n) \in O(g_2(n))$, then: $t_1(n) + t_2(n) \in O(\max\{g_1(n), g_2(n)\})$. Review this proof and on similar lines, prove the following and record a video explaining your proof.

If $t_1(n) \in \Omega(g_1(n))$ and $t_2(n) \in \Omega(g_2(n))$, then prove that: $t_1(n) + t_2(n) \in \Omega(\min\{g_1(n), g_2(n)\})$