CSC196 **Assignment 4** **Fall, 2020**

Due: Monday, December 7, 11AM

This assignment is worth 15% of your final grade

1. The following is a "thought question" and like our previous thought questions there is not a desired unique answer. The question will be graded on your explanations.

   In Professor Nikolov's discussion of differential privacy he mention the claim that 70% of people in the US can be uniquely identfied by the following information: zip code, gender, age.

   - Do you think that a similar % of Canadians can be uniquely identified by postal code, gender, age? If not, would the % be higher or lower. In any case, provide a brief explanation for your answer.
   - Suppose you want to increase the % in the US, say to 80% or more. What one additional piece of information would you add. Explain your answer. (You cannot just say, add the person's name, which would come close to achieving 100%.). Again, give a brief explanation for your answer.

2. In class we showed how to "efficently"' find a certificate for a satisfiable formula if we can "efficiently" decide SAT. (Recall, we are equating "efficient" with polynomial time.)

   Show how to efficiently find a certificate for each of the following problems assuming that the decision problem is efficiently solvable.

   - $SUBSET\text{-}SUM = \{(a_1, \ldots, a_n, t | \exists S : \sum_{a_i \in S} a_i = t\}$
   - $VERTEX\text{-}COLOUR$ as defined in the slides for Week 9.
     Hint: If there is a k colouring of a graph G then any permutation of the colours is still a valid colouring. Now the goal is to colour verttices one by one. In order to have the effect of fixing a colour for a vertex we will need to add additional vertices and edges to the input graph so that these additional vertices require k colours.
   - $FACTOR$ as defined in the slides for week 9.

3. Assume the decision problem $FACTOR$ can be solved in time $O(n^2)$ (by some algorithm in some von Neumann style computer). Estimate a time bound for finding a certificate as in the previous question.

4. Informally argue why $P = NP$ implies one-way functions cannot exist. We will assume that if $f(x)$ is a one-way function, then $|f(x)| = \ell(|x|) \geq |x|$ for some function ℓ.

5. Perhaps one more question to follow