CS46 Lab 11

Lab problems are an opportunity for discussion and trying many different solutions. They are **not counted towards your grade**, and **you do not have to submit your solutions.** The purpose of these lab problems is to get more comfortable with reasoning and writing about asymptotic notation and nondeterministic Turing machine runtimes.

1. Prove the following asymptotic statements.
   - $f(n) = an^2 + bn + c$ for some constants $a, b, c > 0$. Prove that $f(n) = O(n^2)$.
   - $g(n) = 13n^5 - 29n^4 + 11n^2$. Prove that $g(n) = O(n^5)$.
   - $h(n) = 7 - 49n + 343n^7$. Prove that $h(n) = O(n^7)$.
2. **Asymptotic Properties**.
   - Prove that big-O is *transitive*; that is, prove that if $f = O(g)$ and $g = O(h)$ then $f = O(h)$.
   - Prove that is $f = O(h)$ and $g = O(h)$, then $f + g = O(h)$.
   - Is the same true for multiplication? If $f = O(h)$ and $g = O(h)$, what can we say about $f \cdot g$?
3. **Nondeterministic TM Runtime**. Suppose you have a nondeterministic TM N whose runtime is $T_N(n) = t(n)$. Convert this into a deterministic Turing machine M using the procedure we saw earlier in the semester. What is the running time of M?
4. **Polynomial Time Verifiers**. A polynomial time verifier for a language L is a deterministic Turing machine which takes two inputs $\langle w, x \rangle$ such that the following holds:
   - If $w \in L$ then there exists x such that M accepts $\langle w, x \rangle$.
   - If $w \notin L$, then **for all x**, M rejects $\langle w, x \rangle$.
   - M runs in $t(n)$ steps, where n is the length of w and $t(n)$ is some polynomial.

   (a) Argue that if $w \in L$ and $|w| = n$ then there exists some x which causes M to accept such that the length of x is polynomial in n. (e.g. $|x| \leq n^k$ for some constant k).

   (b) Prove that if there is a nondeterministic TM that decides L in polynomial time, then there exists a polynomial-time verifier for L.

   (c) Prove that if L has a polynomial time verifier, then there exists a polynomial-time nondeterministic Turing machine that decides L.
5. A **clique** in an undirected graph is a group of vertices all of which are connected to each other. Let $CLIQUE = \{\langle G, k \rangle | G \text{ is a graph which contains a clique of size } k\}$. Give a polynomial-time verifier for $CLIQUE$.
6. Let $FACTOR = \{\langle N, d \rangle | N \text{ is a positive integer written in binary and d divides N}\}$. Give a polynomial-time verifier for $FACTOR$.
7. Give a polynomial-time verifier for $\overline{FACTOR}$.