CSE 431 Winter 2022
Assignment #6

Due: Thursday February 24, 2022, 11:59 PM

Reading assignment: Read sections 9.3 and 7.5 of Sipser's text.

Problems:

1. (20 points) Let $U = \{\langle M, x, 1^t \rangle \mid M \text{ is an NTM that accepts input } x \text{ within } t \text{ steps}\}$.
   Show that U is NP-complete.
   (Hint: You don't need the Cook-Levin theorem for this question.)

2. (20 points) In class, we saw that almost all Boolean functions $f : \{0,1\}^n \to \{0,1\}$ require circuits of size at least $\Omega(2^n/n)$. In this problem, you will show that this is not too far from optimal for circuits using 2-input $\wedge$ and $\vee$ gates and $\neg$ gates. (Getting a matching upper bound is an extra credit problem below.)

   (a) Show how a (canonical) sum-of-products (equivalently disjunction normal form (DNF)) represention can be used to give a circuit that computes any n-bit function f. Using O notation, what size bound do you get for your circuit as a function of n?

   (b) Improve the previous result and show via induction that there is a constant c such that every $n-$bit Boolean function has a circuit that computes it with at most $c \cdot 2^n$ gates.

3. (20 points) Let ϕ be a 3CNF-formula. An NAE assignment to the variables of ϕ is one that satisfies ϕ but does not set all three literals to true in any clause.

   (a) Show that the negation of an NAE assignment for ϕ is also an NAE assignment for ϕ.

   (b) Let *NAESAT* be the set of all 3CNF formulas ϕ that have an NAE assignment. Prove that *NAESAT* is NP-complete. For the hardness part use a reduction from 3SAT.
   (Hint: Use the function that replaces each clause C_i of ϕ of the form $(y_1 \vee y_2 \vee y_3)$ where y_1, y_2, y_3 are literals by the two clauses $(y_1 \vee y_2 \vee z_i)$ and $(\overline{z_i} \vee y_3 \vee w)$ where w is a single new variable for all clauses and there is one z_i variable per original clause.)

4. (20 points) For any set of people V, an *influential subset* is a set $S \subseteq V$ of people so that everyone in V is either in S, has a friend in S, or both. We can represent the friendship relationships between pairs of people by edges in an undirected graph G with vertices V so we carry over the definition of influential subset to subsets of vertices of such graphs.
   Let $INFLUENTIAL\text{-}SUBSET = \{\langle G, k \rangle \mid G \text{ has an influential subset } S \subseteq V \text{ of size } \leq k\}$.
   Show that $INFLUENTIAL\text{-}SUBSET$ is NP-complete, using the NP-hardness of $VERTEX\text{-}COVER$.
   (Hint: In the reduction from $VERTEX\text{-}COVER$, add vertices and edges to the original graph using precisely one extra vertex per original edge.)

5. (20 points) Let $01ROOT = \{\langle p\rangle \mid p$ is a polynomial in n variables with integer coefficients such that $p(x_1, \ldots, x_n) = 0$ for some assignment $(x_1, \ldots, x_n) \in \{0,1\}^n\}$.

   (a) Show that $01ROOT \in NP$.

   (b) Show that $3SAT \leq_m^P 01ROOT$. (HINT: First figure out how to convert each clause into a polynomial that evaluates to 0 iff the clause is satisfied. Then create a polynomial q that evaluates to 0 if and only if all of its inputs are 0. Finally, figure out how to combine the individual polynomials for the clauses using the polynomial q.

6. (Extra credit) In this problem you will prove the optimality of the $\Omega(2^n/n)$ lower bound on circuit size for computing n-bit Boolean functions. To do this, we generalize our definitions to allow a single circuit that computes multiple functions at once: we simply have multiple nodes designated as output nodes, one per function being computed. Its circuit size remains the total number of gates.

   (a) Let k be the smallest integer such that $2^k \geq n/2$. Show that a single circuit that simultaneously computes all possible Boolean functions on inputs $x_1, ..., x_k$ requires only $O(n \cdot 2^{n/2})$ gates in total.

   (b) Let $\ell \geq k$ and consider any fixed sequence of bits to be assigned to the last $n - \ell$ input positions $b = (b_{\ell+1}, ..., b_n) \in \{0,1\}^{n-\ell}$. To emphasize that these bits are fixed, we define
   $$f_b(x_1, ...x_\ell) = f(x_1, ..., x_\ell, b_{\ell+1}, ..., b_n).$$
   Define the set of functions
   $$\mathcal{F}_\ell := \left\{ f_b(x_1, ..., x_\ell) \;:\; b \in \{0,1\}^{n-\ell} \right\}.$$
   Suppose that you have a single circuit that computes all functions in $\mathcal{F}_{\ell-1}$. Show that you only need an additional $O(2^{n-\ell})$ gates to build a single circuit that computes every function in $\mathcal{F}_\ell$ at once.

   (c) Use the previous two parts to conclude that every Boolean function has a circuit that computes it with $O(2^n/n)$ gates.