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 $U = \{⟨M, x, 1^t⟩ | M$ is an NTM that accepts input $x$ within $t$ 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 $f : \{0, 1\}^n \rightarrow \{0, 1\}$ require circuits of size at least $Ω(2^n/n)$. In this problem, you will show that this is not too far from optimal for circuits using 2-input $∧$ and $∨$ gates and $¬$ 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)) representation 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 $(y_1 \lor y_2 \lor y_3)$ where $y_1, y_2, y_3$ are literals by the two clauses $(y_1 \lor y_2 \lor z_i)$ and $(\overline{z_i} \lor y_3 \lor w)$ 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 $INFLUENTIAL-SUBSET = \{⟨G, k⟩ | G$ has an influential subset $S \subseteq V$ of size $\leq k$\}.
   Show that $INFLUENTIAL-SUBSET$ is NP-complete, using the NP-hardness of $VERTEX-COVER$.
   (Hint: In the reduction from $VERTEX-COVER$, add vertices and edges to the original graph using precisely one extra vertex per original edge.)
5. (20 points) Let \( 01\text{ROOT} = \{ \langle p \rangle \mid p \text{ is a polynomial in } n \text{ variables with integer coefficients such that } p(x_1, \ldots, x_n) = 0 \text{ for some assignment } (x_1, \ldots, x_n) \in \{0, 1\}^n \} \).

(a) Show that \( 01\text{ROOT} \in NP \).

(b) Show that \( 3\text{SAT} \leq^P \text{m} 01\text{ROOT} \). (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 \( x_1, \ldots, x_k \) 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 \( b = (b_{\ell+1}, \ldots, b_n) \in \{0, 1\}^{n-\ell} \). To emphasize that these bits are fixed, we define

\[
 f_b(x_1, \ldots, x_\ell) = f(x_1, \ldots, x_\ell, b_{\ell+1}, \ldots, b_n).
\]

Define the set of functions

\[
 F_\ell := \{ f_b(x_1, \ldots, x_\ell) : b \in \{0, 1\}^{n-\ell} \}.
\]

Suppose that you have a single circuit that computes all functions in \( F_{\ell-1} \). Show that you only need an additional \( O(2^{n-\ell}) \) gates to build a single circuit that computes every function in \( F_\ell \) 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.