Theory of Computation

Midterm Examination on November 18, 2022
Fall Semester, 2022

Problem 1 (15 points) Recall that the **depth** of a gate g is the length of the longest path in a circuit from g to an input gate. A circuit is **leveled** if every input of a gate in depth k comes from one in depth $k-1$. LEVELED CIRCUIT asks if a leveled circuit is satisfiable. Prove that LEVELED CIRCUIT is NP-complete. (No need to show that it is in NP.)

Proof: We can obtain a leveled circuit from any circuit C by increasing the number of gates by a polynomial factor, as follows. This holds for the input gates. Inductively, suppose that all gates of depth $k-1$ have length $k-1$ for the shortest paths to the input gates. Now consider gates of depth k. Pick any gate g with a shorter shortest path to the input gates, say length $l < k$. Insert a series of $k-l$ $\vee$ gates on the edge between g and its predecessor gate on one such path. These $k-l$ $\vee$ gates have their two identical inputs. Note that $k-l = O(|\, C \,|)$. So they act as the identity function. The new circuit has size $O(|\, C \,|^2)$. Finally, recall that LEVELED CIRCUIT is NP-complete by Cook's Theorem. ■

Problem 2 (15 points) It is known that 3SAT is NP-complete. Reduce 3SAT to 4SAT to show that 4SAT is NP-hard.

Proof: Let ϕ be an instance of 3SAT, and x, y, z be any boolean variables. We convert ϕ to a 4SAT instance ϕ' by turning each clause $(x \vee y \vee z)$ in ϕ to $(x \vee y \vee z \vee h) \wedge (x \vee y \vee z \vee \neg h)$, where h is a new boolean variable. It can be done in polynomial time.

- (If) If a given clause $(x \vee y \vee z)$ is satisfied by a truth assignment, then $(x \vee y \vee z \vee h) \wedge (x \vee y \vee z \vee \neg h)$ is satisfied by the same truth assignment with h arbitrarily set. Thus if ϕ is satisfiable, ϕ' is satisfiable.
- (Only if) Suppose that ϕ' is satisfied by a truth assignment T. Then $(x \vee y \vee z \vee h) \wedge (x \vee y \vee z \vee \neg h)$ must be true under T. As h and $\neg h$ assume different truth values, $(x \vee y \vee z)$ is true under T as well. Thus ϕ is satisfiable.

■

Problem 3 (15 points) Let $G = (V, E)$ be an undirected graph and K be a positive integer. LONGEST PATH ask if there is a simple path which contains at least K edges in G. Show that LONGEST PATH is NP-complete. (You need to show that LONGEST PATH is in NP.)

Proof: We first show that LONGEST PATH is in NP. Given an instance G, we guess a set of edges of size at least K and at most $|E|$ and examine if it is a simple path in G. This can be done in polynomial time. We proceed to show that LONGEST PATH is NP-hard by reducing HAMILTONIAN PATH to LONGEST PATH. Given an instance G' of HAMILTONIAN PATH, we create an instance (G, K) of LONGEST PATH as follows: Take $G = G'$ and set $K = |V| - 1$. Then there exists a simple path of length K in G if and only if G' contains a Hamiltonian path. ■

Problem 4 (20 points) Prove that 3SAT formulas are less expressive than CNFs in the sense that there are n-variable boolean functions which can be expressed by n-variable CNF formulas but not by n-variable 3SAT ones.

Proof: CNFs can express 2^{2^n} boolean functions in n variables. For 3SAT formulas, each literal in a clause has $2n$ choices; hence there are at most $(2n)^3$ different clauses. A clause can be either picked or not to form a 3SAT formula. So 3SAT formulas can only express at most $2^{(2n)^3}$ boolean functions in n variables. ■

Problem 5 (15 points) Calculate $\phi(313716)$ and $77^{192960} \mod 313716$. (You need to write down the calculation detail explicitly.)

Proof:

- Factorize $373716 = 2^2 \times 3 \times 13 \times 2011$. Hence $\phi(313716) = 313716 \times \frac{1}{2} \times \frac{2}{3} \times \frac{12}{13} \times \frac{2010}{2011} = 94680$.
- By the Fermat-Euler theorem (Corollary 63),

$$(77^{94680})^2 = 77^{94680} = 1 \mod 313716.$$

■

Problem 6 (20 points) Let $G = (V, E)$ be an undirected graph and K be a positive integer. The problem UNREACHABILITY asks if there does not exist a simple path of length at least K from node u to v in G. Prove that UNREACHABILITY is coNP-complete.

Proof: Recall that L is NP-complete if and only if its complement $\bar{L} = \Sigma^* - L$ is coNP-complete. We only need to prove that its complement problem REACHABILITY is NP-complete. REACHABILITY asks if there exists a simple path of length at least K from node u to v. It is clear that REACHABILITY is in NP: guess a simple path of length at least K from node u to v and verify it in polynomial time. Recall that HAMILTONIAN PATH is NP-complete. Clearly, there exists a Hamiltonian path from u to v in G if and only if there exists a simple path of length K from u to v in G. Hence the reduction from HAMILTONIAN PATH produces G and $K = |V| - 1$. ■