1 Primality in NP

Let PRIMES be the set of prime numbers. It is easy to see that PRIMES ∈ coNP since a certificate for non-primality (e.g., for being composite) of n is a factoring n = ab for a, b ∈ {2, . . . , n − 1}. In this problem, we will prove that also PRIMES ∈ NP, e.g., there is a certificate for being prime which can be verified in polynomial time. This made PRIMES be one of the few problems we knew in NP ∩ coNP. However, in the breakthrough work of Agrawal-Kayal-Saxena [AKS04] in 2004 they proved that in fact PRIMES ∈ P, e.g., they gave a deterministic poly-time algorithm to check if a number is prime or not.

Prove: PRIMES ∈ NP. You may assume the following simple fact in number theory: A number n is prime if there exists a ∈ {2, . . . , n − 1} satisfying a^{n−1} = 1 (mod n) but a^{(n−1)/q} ≠ 1 (mod n) for all prime factors q of n − 1. Note that the length of the proof and the running time of the verifier should be at most polynomial in the input length, that is at most (log(n))^{O(1)}.

2 Graph coloring

A c-coloring of an undirected graph G = (V, E) is a map χ : V → {1, . . . , c} so that adjacent vertices (u, v) get different colors, χ(u) ≠ χ(v). Let

\[ c - COLORING = \{\text{Graphs G which can be c-colored}\} \]

(i) Prove that 3-coloring is NP-complete.

(ii) Prove that 2-coloring is in P.

(iii) Prove that 2-coloring is in fact in LOGSPACE. You may use Reingold’s theorem [Rei05] that undirected connectivity (e.g., checking for an undirected graph G and vertices s, t if there is a path between s and t) is in LOGSPACE.

(iii) Let G be a graph which is 3-colorable. Find a poly-time algorithm which colors G with as few colors as you can. What is the best you can do?
3 Size blowup

Let $\text{EXP} = \cup_{c \geq 1} \text{TIME}(2^{n^c})$ and $\text{NEXP} = \cup_{c \geq 1} \text{NTIME}(2^{n^c})$ be the classes of deterministic exponential time, and nondeterministic exponential time, respectively. Prove that if $P = NP$ then $\text{EXP} = \text{NEXP}$.

4 Union and intersection of NP

(i) Let $L_1, L_2 \in NP$. Is $L_1 \cup L_2 \in NP$? Is $L_1 \cap L_2 \in NP$? prove or give a counter-example.

(ii) Let $L_1, L_2$ be NP-complete. Is $L_1 \cup L_2$ NP-complete? Is $L_1 \cap L_2$ NP-complete? prove or give a counter-example.

References
