Homework 6

Problem 1. Prove that if P = NP, then NP = coNP.

Solution. From the homework last week, we have proved that a problem $A \in$ P $\iff$ $\overline{A} \in$ P. From the definition, we have coNP $= \{\overline{A} \mid A \in$ NP$\}$, so if P = NP, then coNP $= \{\overline{A} \mid A \in$ P$\}$. And this results in coNP = P = NP.

Problem 2. For every 2-SAT instance φ of n variables, define graph G_φ of $2n$ vertices as follows. For each variable x_i in φ, G_φ has two vertices labeled by x_i and $\neg x_i$ respectively. There is a directed edge $\ell_i \to \ell_j$ if $(\neg \ell_i) \vee \ell_j$ or $\ell_j \vee (\neg \ell_i)$ is a clause of φ. For notational convenience, for literal $\ell_i = \neg x_{k_i}$, $\neg \ell_i$ is defined to be x_{k_i}. Prove that φ is unsatisfiable if and only if there exist paths from x_j to $\neg x_j$ and from $\neg x_j$ to x_j in G_φ for some j. Use the above fact to show that 2-SAT $\in$ P.

Solution. Suppose φ is unsatisfiable, then for every assignment of variables, there must be two chains of clauses that coerce the assignment of x_j to be true and false respectively. For example,

$$(\neg x_j) \vee l_{k_1}, (\neg l_{k_1}) \vee l_{k_2}, \cdots, (\neg l_{k_{m-1}}) \vee (\neg x_j),$$

and

$$x_j \vee l_{p_1}, (\neg l_{p_1}) \vee l_{p_2}, \cdots, (\neg l_{p_{t-1}}) \vee x_j,$$

where l_{k_i} and l_{p_i} are variables x_t or its negation $\neg x_t$. The former chain ensures that $x_j =$ false, and the latter chain ensures that $x_j =$ true, which leads to a contradiction so that φ is unsatisfiable. From the first chain, we can see that there must be an edge from x_j to l_{k_1}, from l_{k_1} to l_{k_2}, $\cdots$, from $l_{k_{m-1}}$ to $\neg x_j$, forming a path from x_j to $\neg x_j$. And from the second chain, we can see that there must be an edge from $\neg x_j$ to l_{p_1}, from l_{p_1} to l_{p_2}, $\cdots$, from $l_{p_{t-1}}$ to x_j, forming a path from $\neg x_j$ to x_j.

    Suppose there exist paths from x_j to $\neg x_j$ and from $\neg x_j$ to x_j in G_φ. Note that the path from x_j to $\neg x_j$ ensures that $x_j =$ false, because of the following chain:

$$(\neg x_j) \vee l_{k_1}, (\neg l_{k_1}) \vee l_{k_2}, \cdots, (\neg l_{k_{m-1}}) \vee (\neg x_j),$$

where l_{k_i} is a variable x_t or its negation $\neg x_t$. Similarly, the path from $\neg x_j$ to x_j ensures that $x_j =$ true, which is a contradiction. Then φ is unsatisfiable.

Therefore, φ is unsatisfiable if and only if there exist paths from x_j to $\neg x_j$ and from $\neg x_j$ to x_j in G_φ for some j. It is easy to see that the existence of such paths can be checked in polynomial time, for we can use breadth-first search, starting from a vertex x_j, to find whether there is a path from x_j to $\neg x_j$ and vice versa. Thus, 2-SAT $\in$ P.

Problem 3. The Lehmer's theorem states that a natural number n is a prime number if and only if the following two conditions hold:

1. There is number a such that $a^{n-1} \equiv 1 \pmod{n}$.

2. For every prime factor q of $n - 1$, $a^{(n-1)/q} \not\equiv 1 \pmod{n}$.

Use this theorem to show that PRIME $\in$ NP $\cap$ coNP. (Hint: To prove PRIME $\in$ NP, you may need to use recursively defined witness.)

Solution. We first prove that PRIME $\in$ NP. Given a number a and the prime factorization of $n - 1$, we can verify in polynomial time:

1. $a^{n-1} \equiv 1 \pmod{n}$. This is because we can calculate $a^{n-1} \mod n$ in $O(\log n)$ time by exponentiation by squaring.

2. for every prime factor q of $n - 1$, $a^{(n-1)/q} \not\equiv 1 \pmod{n}$. This is because we can calculate $a^{(n-1)/q} \mod n$ in $O(\log n)$ time by exponentiation by squaring, Also, there are only $O(\sqrt{n})$ such factor q for $n - 1$, because factors appear in pairs. If one of the factor is greater than $\sqrt{n-1}$, then the other one must be less than $\sqrt{n-1}$. And an upper bound of the number of factors that $n - 1$ have is $O(\sqrt{n})$, because $n - 1$ can only have $\sqrt{n-1}$ factors that are the 'smaller ones.'

Therefore, PRIME $\in$ NP.

Then we prove that PRIME $\in$ coNP. Suppose n is not a prime number and given k where $k \mid n$, then we can verify this in polynomial time. Therefore, PRIME $\in$ coNP.

In conclusion, PRIME $\in$ NP $\cap$ coNP.