1. Suppose there exists a language A∈NP that is not NP complete, but satisfy the property that for all B∈NP, B∈P^A, then can we conclude that P≠NP? Justify. 3

   Soln: If P=NP, then any two non-trivial problems in NP are reducible to each other (under any notion of polynomial time reduction).

2. If the graph isomorphism problem GI is NP complete and AM⊆NP, then can we conclude that NP=coNP? Justify your answer. 3

   Soln: GI is NP complete ⇒ GNI is co-NP complete. AM⊆NP ⇒ coNP⊆NP ⇒ NP=coNP.

3. Let $L \in$ BPP. Let $A(x,r)$ be a polynomial time BPP verifier for L that uses $m = poly(n)$ random bits on input x of length n, such that $Pr_r(A(x,r) \neq (x \in L)) \leq \frac{1}{2^n}$. Suppose $x \in L$, $|x| = n$. Let $z_1, z_2, .., z_m$ be randomly chosen from $\{0,1\}^m$. Show that the probability that there exists an $r \in \{0,1\}^m$ such that $A(x, r \oplus z_i) = 0$ for all $1 \leq i \leq m$ is strictly less than 1. 3

   Soln: Fix any r. $Pr(A(x, z_1 \oplus r) = 0 < \frac{1}{2^n}$ for each i. Thus, $Pr(\forall i A(x, z_i \oplus r)) == (\frac{1}{2^n})^m = \frac{1}{2^{mn}}$. Now, this is for any particular r. Probability that at least for one r(among 2^m possibilities of r), $\bigwedge_i A(x, r \oplus z_i) = 0$ is an event of probability at most $2^m(\frac{1}{2^{mn}}) < 1$. (Additonal Note: A consequence of this observation is that if $x \in L$, there exists $z_1, z_2, ..z_m$ such that $\bigvee_i A(x, r \oplus z_i) = 1$ for all $r \in \{0,1\}^m$).

4. If we are designing an MA protocol for a language L∈BPP with algorithm $A(x,r)$ specified in the previous question, then what must be the proof sent by Merlin to Arthur? What is the verification step done by Arthur? 3

   Soln: Assume that $Pr(A(x,r) \neq (x \in L)) = \frac{1}{2^n}$. Merlin can choose $z_1, z_2, ..z_m$ specified in the Additional note in the solution to the previous question to Arthur. Aruther choses a random r and tests $\bigvee_i A(x, r \oplus z_i) = 1$. If $x \in L$, proper choice of $z_1, ..z_m$ by Merlin ensures that Arthur will accept. If $x \notin L$, since r is randomly chosen, $A(x, z_i \oplus r) = 1$ with probability at most $\frac{1}{2^n}$ for each i. Hence the probability that for some i $A(x, z_i \oplus r) = 0$ is bounded by (the union bound) $\frac{m}{2^n} < 1$ as $m = poly(n)$ for n large enough.

5. If MA⊆ P/POLY, can we conclude that PH collapses? If so, to which level? 3

   Soln: Since NP⊆MA (the verifier can get the certificate from Merlin and do the verification without even doing coin tosses, achieving zero error), if MA⊆P/POLY, we have PH=Σ_2^p by Karp Lipton Theorem.

6. Suppose we have an MA proof system for a language L where, given input string x, Merlin sends Arthur a proof y for membership for x in L and Arthur guesses an m bit random string r and runs a verifier $A(x,y,r)$ which accepts with probability 1 when $x \in L$ and accepts with probability less than $\frac{1}{2^{m+1}}$ when $x \notin L$. Design an AM protocol for accepting L and prove the soundness and completeness of your protocol. 3

   Soln: Arthur picks $r \in \{0,1\}^m$ and sends to Merlin. Merlin sends the proof y and Arthur runs $A(x,y,r)$. A randomly chosen r has probability at most $\frac{1}{2^{m+1}}$ to be "bad" for any fixed y (in that $A(x, y_1, r)$ gives the wrong answer). Thus, the probability that r is bad for at least one y is at most $\frac{2^k}{2^{m+1}}$, where k is the length of each proof y. If this quantity is less than 1, we have an AM protocol. We can set (through probability amplification) the value of m to meet the requirment $m = k$.

7. Show that AM⊆ Π_2^p. 3

   Soln: $L \in$AM if there exists a polynomially balanced $A(x,y,r)$ such that: a) $x \in L \Rightarrow \forall r \exists y A(x,y,z) = 1$. (This is a Π_2^p condition). b) if $x \notin L$, $Pr_r(\exists y A(x,y,z) = 1) < \frac{1}{2}$. Since the probability for a particular r to satisfy $\forall y A(x,y,r) = 0$ is greater than 0, we conclude that $\exists r \forall y A(x,y,r) = 0$, which is a Π_2^p condition.

8. A symbolic $n \times n$ matrix $A = (x_{ij})$ has its $(i,j)^{th}$ entry set to either the indeterminate (variable) x_{ij} or zero. The symbolic determinant problem (SYMDET) takes as input a symbolic $n \times n$ matrix A and decides whether Det(A)=0. Show that the problem of testing whether an (n,n) bipartite graph has a perfect matching is log-space reducible to SYMDET. $\boxed{3}$

   Soln: Consider the matrix A with $A(i,j) = x_{ij}$ if (i,j) is an edge in G, 0 otherwise. It is easy to see that the graph has determinant zero if and only if there is no perfect matching in G.

9. Let M^B be a deterministic Turing machine that queries an oracle for a language B and runs for at most n^k steps on any input of length n. For any language B, define $L_B = \{1^n : B$ contains at least one string of length $n\}$. Design a language B such that $L(M^B) \neq L_B$. $\boxed{3}$

   Soln: Choose n_0 such that $2^{n_0} > n^k$. Define B as follows: B is either empty or contains at most one string, and that too of length exactly n_0. Consider the string 1^{n_0} of length n_0. We will define B in such a way that $M^B(1^{n_0}) = 1$ if and only if B is empty, thereby ensuring that $L(M^B) \neq L_B$. Suppose M on input 1^{n_0} querires strings $x_1, x_2, ..., x_t$ ($t \leq n_0^k$) to its oracle B, we will define B not to contain any of the strings $x_1, x_2, ..x_t$ so that the answer supplied by the oracle is always 0. Finally, if $M^B(1^{n_0})$ accepts, we set $B = \emptyset$ and hence $1^{n_0} \notin L_B$. Otherwise, let x be any string in $\{0,1\}^{n_0}$ different from $x_1, x_2, ..x_t$ (such x must exist because $2^{n_0} > n^k$). Let $B = \{x\}$. Now $L_B = \{1^{n_0}\} \neq L(M^B)$.

10. Let $R \subseteq \Sigma^* \times \Sigma^*$ be a polynomially balanced binary relation. Define the decision problem $L_R = \{x : \exists y R(x,y) = 1\}$ and $\#R(x) = |\{y : R(x,y) = 1\}|$. Suppose it is true that for all polynomially balanced R, $\#R \in P^{L_R}$ (that is, the certificate counting problem is Turing reducible to the certificate existence problem for all languages in NP). Then show that P=NP. $\boxed{3}$

    Soln: for any R, $\#R \preceq_m^p \#$PM, where #PM is the problem of counting the number of perfect matchings in a bipartite graph (Valiant's theorem). However, the decision problem PM of checking whether a graph contains a perfect matching is indeed in P. Hence, under the assumption in the question, #PM$\in P^{PM} = P$. As #PM is #P complete, this would mean #P$\subseteq$ P, which in turn would imply P=NP.

11. Show that there exists a directed graph G and vertices $s, t \in V(G)$ such that $s - t$ path exists in G, but a random walk in G starting s may fail to reach t with positive probability. (This shows that the RL algorithm for $s - t$ REACH on undirected graph will not work with directed graphs). $\boxed{3}$

    Soln: In the graph $G(V,E)$ with $V = \{1,2,3\}$ and $E = \{(1,2)(1,3)\}$, it is easy to see that a random walk starting at 1 will visit only one of 2 and 3, each case happening with probability $\frac{1}{2}$.

12. A (cryptographic) one way function is a polynomial time computable $f : \Sigma^* \longrightarrow \Sigma^*$ such that the problem of computing f^{-1} is hard. That is, given any $y \in \Sigma^*$, the problem of finding an x such that $f(x) = y$ is not polynomial time computable. Show that if one way functions exist, then P$\neq$NP. $\boxed{3}$

    Soln: Given y, a non-deterministic Turing machine can guess x and hence f^{-1} is in NP. Thus, if P=NP, inversion will not be hard.

13. Show that $S_2^p \subseteq \Sigma_2^p \cap \Pi_2^p$. $\boxed{3}$

    Soln: By definition of S_2^p, $x \in L \Rightarrow \exists y \forall z, P(x,y,z) = 1$ This is a Σ_2^p condition. Further, $x \notin L \Rightarrow \exists z \forall y, P(x,y,z) = 0$, which implies the Σ_2^p requirement $\forall y \exists z P(x,y,z) = 0$, and consequently $S_2^p \subseteq \Sigma_2^p$. The proof for $S_2^p \subseteq \Pi_2^p$ is similar.