Problem 1

In this problem you will show that if we don't put reasonable restrictions on the class of ensembles, average-case complexity is no easier than worst-case complexity.

(a) Show that for every $L \notin \mathrm{P}$ there exists an ensemble μ_L such that (L, μ_L) does not have polynomial-time heuristic algorithms. (**Hint:** μ_L should give a lot of weight to the "hard" instances of L.)

(b) Show that there exists an ensemble μ such that for every $L \in \mathrm{NP}$, (L, μ) has polynomial-time heuristic algorithms if and only if $L \in \mathrm{P}$. (**Hint:** Use the various μ_L from part (a) to construct μ.)

Problem 2

In this problem you investigate the difference between polynomial-time computable and polynomial-time samplable ensembles.

(a) Let $\{G_n\}$ be a pseudorandom generator. Show that the ensemble μ obtained by choosing a random $X \in \{0,1\}^n$ and outputting $G_n(X)$ is not polynomial-time computable. Thus if pseudorandom generators exist, then $\mathrm{PC{\small OMP}} \neq \mathrm{PS{\small AMP}}$.

(b) Show that $\mathrm{PC{\small OMP}} = \mathrm{PS{\small AMP}}$ if and only if $\mathrm{P} = \mathrm{P}^{\#\mathrm{P}}$. (**Hint:** For the "only if" direction, consider sampling pairs (φ, a), where φ is a DNF and a is a satisfying assignment for φ.)

Problem 3

Show that (L, μ) has an average polynomial-time algorithm if and only if there is an algorithm A with the following properties:

- A takes two inputs x and ε and runs in time $\mathrm{poly}(|x|, 1/\varepsilon)$.
- For every input x and every ε, $A(x, \varepsilon)$ outputs either $L(x)$ ("yes" if $x \in L$, "no" if $x \notin L$) or the special symbol "fail".
- For every n and ε,
$$\Pr[A(x, \varepsilon) = \text{"fail"}] \leq \varepsilon.$$

Using this alternative definition of average polynomial-time algorithms, conclude that if (L, μ) reduces to (L', μ') and (L', μ') has an average polynomial-time algorithm, so does (L, μ).

Problem 4

An undirected graph is *bipartite* if it has no cycles of odd length. We define the decision problem

$$BIPART = \{G : G \text{ is bipartite}\}.$$

Assuming that $USTCON \in \mathrm{L}$, show that $BIPART \in \mathrm{L}$. Recall the decision problem $USTCON$:

$$USTCON = \{(G, s, t) : s \text{ and } t \text{ are connected in } G\}.$$

(**Hint:** Look at the graph G^2 whose vertices are the same as G and whose edges correspond to paths of length two in G.)