Tutorial 10:

A1: Suppose L_1 and L_2 in PP is witnessed by M_1 and M_2 respectively. Consider $M(x)$, which runs $M_1(x)$ and $M_2(x)$ and accepts iff exactly one of $M_1(x)$ and $M_2(x)$ accepts. Then, $M(x)$ is correct if both $M_1(x)$ and $M_2(x)$ are correct outputs, or both are wrong outputs. Thus, M is correct with probability $(1/2+\alpha_1)(1/2+\alpha_2)+(1/2-\alpha_1)(1/2-\alpha_2) = 1/2+2\alpha_1\alpha_2 > 1/2$, where $M_1(x)$ is correct with probability $1/2+\alpha_1$ and $M_2(x)$ is correct with probability $1/2+\alpha_2$.

A2: It is easy to verify that QBF is in PSPACE (details left to the student).

To show that QBF is PSPACE-hard, suppose L is a PSPACE language as witnessed by Turing Machine M which is n^k space bounded, and 2^{n^k} time bounded (being c^{n^k} time bounded can be done similarly).

Let $P_m(U,V)$ denote the formula for saying that the machine M can go from ID U to ID V in at most 2^m steps.

P_0 is easy to define.

$P_{m+1}(U,V) = (\exists Z)(\forall X)(\forall Y)[[(U = X \text{ and } Y = Z) \text{ or } (Z = X \text{ and } Y = V)] \Rightarrow P_m(X,Y)]$

equivalently:

$P_{m+1}(U,V) = (\exists Z)(\forall X)(\forall Y)[[\neg(U = X) \text{ and } \neg(Z = X)] \text{ or } [\neg(U = X) \text{ and } \neg(Y = V)] \text{ or } [\neg(Y = Z) \text{ and } \neg(Z = X)] \text{ or } [\neg(Y = Z) \text{ and } \neg(Y = V)] \text{ or } P_m(X,Y)]$

Suppose $U = u_1u_2\ldots u_{n^k}$, $V = v_1v_2\ldots v_{n^k}$, $X = x_1x_2\ldots x_{n^k}$, $Y = y_1y_2\ldots y_{n^k}$, $Z = z_1z_2\ldots z_{n^k}$. Now, for example, $\neg(U = X)$ and $\neg(Z = X)$ can be expressed as disjunction of n^{2k} formulas (for $1 \le i,j \le n^k$) as follows.

$(\neg u_i$ and x_i and $\neg z_j$ and $x_j)$ or $(\neg u_i$ and x_i and z_j and $\neg x_j)$ or $(u_i$ and $\neg x_i$ and $\neg z_j$ and $x_j)$ or $(u_i$ and $\neg x_i$ and z_j and $\neg x_j)$.

The quantifiers in $P_m(X,Y)$ can be brought forwards to the beginning using standard methods. Thus, we can express $P_m(X,Y)$ in prenex form in length polynomial in m, n.

Now, $x \in L$ iff $P_{n^k}(SID, AID)$, where SID is starting ID and AID is accepting ID for M on input x.