COMPLEXITY: Exercise No. 8
partial solutions

1 Question 1

Prove that if there is a PH-complete problem, then $PH = \Sigma_k$ for some constant k.
Answer: Suppose L is PH-complete. Then $L \in \Sigma_k$ for some k. For all $L' \in PH$, there is a reduction from L' to L, thus L' is in Σ_k, too.

2 Question 2

Prove that if $PH = PSPACE$ then $PH = \Sigma_k$ for some constant k.
Answer: Implied by the previous question and the fact that there is a $PSPACE$-complete problem (for example, TQBF).

3 Question 3

Prove that $RP \subseteq NP$.
Answer: We can look at a probabilistic TM as an NDTM. In the case of RP, if x is not in the language of the TM, then there is no accepting path, and if x is in the language then we accept with probability at least $\frac{1}{2}$, so there is at least one accepting path.

4 Question 4

Prove that $NP \subseteq PP$.
Answer: Let $L \in NP$ and let M be an NDTM for L. We construct a probabilistic TM M' for L as follows. Whenever M has more than one possible transition, M' chooses one of them randomly. Thus if $x \notin L$, $Pr[M'(x) = T] = 0$, and if $x \in L$, $Pr[M'(x) = T] > 0$. In order to turn M' into a PP TM, we add another coin toss at the beginning. With probability $\frac{1}{2}$ we return TRUE immediately, and with probability $\frac{1}{2}$ we continue as described above. Thus, if $x \notin L$, $Pr[M'(x) = T] = \frac{1}{2}$, and if $x \in L$, $Pr[M'(x) = T] > \frac{1}{2}$.

5 Question 5

Consider the following alternative definition of ZPP:
$L \in ZPP$ iff there exists a probabilistic polynomial time TM M that answers TRUE,FALSE or QUIT, and:

- If $x \in L$ then M always returns TRUE or QUIT.
- If $x \notin L$ then M always returns FALSE or QUIT.

- $\forall x \;\; Pr[M(x) = QUIT] \leq \frac{1}{2}$.

Prove that this definition is equivalent to the definition we saw in class.
Answer:

- Let $L \in ZPP$ according to the definition from class, and let M be an appropriate TM. Suppose that the expected running time of M is $p(n)$. We construct a TM M' that runs M, and if M does not halt after $2p(n)$ steps it halts and returns QUIT. Otherwise it returns the answer of M. M' clearly runs in polynomial time, and always returns the correct answer or QUIT, and for all x, the probability that M' returns QUIT is the probability that M runs more than $2p(n)$ steps, which is, by Markov's inequality, at most $\frac{1}{2}$.

- Let $L \in ZPP$ according to the above definition, and let M be an appropriate TM. Suppose that M runs in time $p(n)$. We construct a TM M' that runs M over and over until the first time it returns a non-QUIT answer. Obviously, M' always returns the correct answer. The number of times M' runs M until it returns a non-quit answer is a geometric random variable with parameter $p \geq \frac{1}{2}$. Thus its expected value is at most 2, and therefore the expected running time of M' is at most $2p(n)$.

6 Question 6

Prove that $RP \cap co - RP \subseteq ZPP$.
Answer: Let $L \in RP \cap co - RP$. Let M_1 be an RP TM for L, and let M_2 be an RP TM for L^c. We construct a probabilistic TM for L as follows. Given an input x, run M_1 and M_2 on x. If $x \in L$ then $M_1(x)$ is TRUE with probability at least $\frac{1}{2}$, and $M_2(x)$ is always FALSE, and if $x \notin L$ then $M_2(x)$ is TRUE with probability at least $\frac{1}{2}$, and $M_1(x)$ is always FALSE. Thus, if one of these TM's returns TRUE M will return the correct answer accordingly, and if they both return FALSE M will return QUIT. It is easy to check that M is a ZPP machine for L according to the definition from the previous question.