Problem 1

Proof. For every $x, x' \in \{0, 1\}^n$, $x \neq x'$ and for every $y, y' \in \{0, 1\}^k$

\[
\Pr_{h \in R_{A,b}}[h(x) = y \land h(x') = y'] = \Pr_{A,b}[Ax + b = y \land Ax' + b = y'].
\]

Let $A = [a_1, a_2, a_3, \ldots, a_k]^T$. As $x \neq x'$, without loss of generality, assume $x_j = 0, x_j' = 1$. We know that $Pr[a_i x + b_i = y_i] = 1/2$. Also

\[
Pr[a_i x' + b_i = y_i' | a_i x + b_i = y_i] = 1/2,
\]

because the $j$-th entry of $a_i$, saying $a_{i,j}$, is uniform. So

\[
Pr[a_i x' + b_i = y_i' \land a_i x + b_i = y_i] = 1/4.
\]

As $(a_1, b_1), (a_2, b_2), \ldots, (a_k, b_k)$ are independent, $Pr_{A,b}[Ax + b = y \land Ax' + b = y'] = 1/2^{2k}$.

So $R_{A,b}$ is a pairwise independent hash function family.

\[
\square
\]

Problem 2

Proof. Let $n$ be the length of the random string sent by the verifier.

Note $AM[2]$ is a public coin protocol. If $x \notin L$ then by the soundness property, for at least 2/3 fraction of strings in $\{0, 1\}^n$ sent by the verifier, no matter what string the prover replies, the verifier will output 0. This is because if there is any reply that can make the verifier output 1, the verifier can just send that reply. Let these strings form the set $A \subseteq \{0, 1\}^n$. Thus $|A| \geq \frac{2}{3}2^n$.

When repeating the protocol for $k$ times, let $S_1, S_2, \ldots, S_k$ be the random strings sent by the verifier. Thus the verifier will output 1 for all $k$ protocols only if $\forall i \in [k], S_i \notin A$. This happens with probability at most $(1/3)^k$ since the $S_i$’s are independent.

\[
\square
\]

Problem 3

Proof. The total number of permutations over $n$ vertices is $n!$. For each such permutation $P$ applied to $G_1$, we obtain some graph $G_0 = P(G_1)$. Since $G_1$ and $G_2$ are isomorphic, we know that there exists a permutation $P'$ over $n$ vertices such that $G_1 = P'(G_2)$. Thus we get that $G_0 = P(P'(G_2)) = P \circ P'(G_2)$. Note that $P \circ P'$ is another permutation over $n$ vertices. Furthermore, if $P_1$ and $P_2$ are two different permutations, then so are $P_1 \circ P'$ and $P_2 \circ P'$. Thus, the function $P \rightarrow P \circ P'$ is a bijection from the set of permutations to itself, where for any permutation $P$, $P'(G_1)$ and $P \circ P'(G_2)$ are the same graph. Therefore, a random permutation applying to $G_1$ or $G_2$ will result in the same distribution.

\[
\square
\]
Problem 4

Proof. We know that $3\text{SAT}$ is in $\text{coNP}$. For any language in $\text{NP}$, we know it is polynomial-time reducible to $3\text{SAT}$. Thus it is also polynomial-time reducible to $3\text{SAT}$. So $\text{NP} \subseteq \text{coNP}$.

For any language $L \in \text{coNP}$, $L \in \text{NP} \subseteq \text{coNP}$. Hence $L \in \text{NP}$. So $\text{coNP} \subseteq \text{NP}$.

Thus $\text{coNP} = \text{NP}$.

By Theorem 5.4 part 1 in the required textbook (proved in Problem 5), as $\Pi_i^p = \text{coNP} = \text{NP} = \Sigma_i^p$, $\text{PH} = \text{NP}$.

\[\square\]

Problem 5

Proof. (1) We use induction to show that for any integer $j \geq i$, $\Sigma_j^p = \Sigma_i^p$.

For the base case $\Sigma_i^p = \Sigma_i^p$ is obvious.

Assume $\Sigma_j^p = \Sigma_i^p$ for some integer $j \geq i$, we show that $\Sigma_{j+1}^p = \Sigma_i^p$.

By definition of $\Sigma_{j+1}^p$, if a language $L$ is in $\Sigma_{j+1}^p$, then there exists a polynomial-time TM $M$ and a polynomial $q$ such that

\[x \in L \iff \exists u_1 \in \{0,1\}^{|x|} \forall u_2 \in \{0,1\}^{|x|} \cdots Q_{j+1}u_{j+1} \in \{0,1\}^{|x|} M(x, u_1, u_2, \ldots, u_{j+1}) = 1\]  

where $Q_k$ denotes $\forall$ or $\exists$ depending on whether $k$ is even or odd, respectively.

Define the language $L'$ as follows:

\[\langle x, u_1 \rangle \in L' \iff \forall u_2 \in \{0,1\}^{|x|} \cdots Q_{j+1}u_{j+1} \in \{0,1\}^{|x|} M(x, u_1, u_2, \ldots, u_{j+1}) = 1.\]

Thus

\[x \in L \iff \exists u_1 \in \{0,1\}^{|x|} \langle x, u_1 \rangle \in L'.\]

By definition $L' \in \Pi_i^p$. So $L' \subseteq \Sigma_j^p = \Sigma_i^p$. So $L' \in \Sigma_i^p$. That is, there exists a TM $M'$ and a polynomial $q'$ such that

\[\langle x, u_1 \rangle \in L' \iff \exists u_2 \in \{0,1\}^{|x|} \cdots Q_{i+1}u_{i+1} \in \{0,1\}^{|x|} M'(x, u_1, u_2, \ldots, u_{i+1}) = 1,\]

where $Q_k'$ denotes $\forall$ or $\exists$ depending on whether $k$ is odd or even, respectively.

This means

\[x \in L \iff \exists u_1 \in \{0,1\}^{|x|} \exists u_2 \in \{0,1\}^{|x|} \cdots Q_{i+1}u_{i+1} \in \{0,1\}^{|x|} M'(x, u_1, u_2, \ldots, u_{i+1}) = 1.\]

By combining $\exists u_1 \in \{0,1\}^{|x|}$ and $\exists u_2 \in \{0,1\}^{|x|}$ into $\exists(u_1, u_2) \in \{0,1\}^{|x|+|y|}$, we see that

$L \in \Sigma_i^p$. Thus $\Sigma_{j+1}^p \subseteq \Sigma_i^p$. Hence $\Sigma_{j+1}^p = \Sigma_i^p$.

(2) For the reverse direction, we first show that $\Pi_i^p \subseteq \Sigma_i^p$. For any language $L \in \Pi_i^p$, we know that

$L \in \Sigma_{i+1}^p$ (since $\Pi_i^p \subseteq \Sigma_{i+1}^p$). As $\Sigma_{i+1}^p \subseteq \text{PH} = \Sigma_i^p$, $L \in \Sigma_i^p$.

Then we show $\Sigma_i^p \subseteq \Pi_i^p$. For any language $L \in \Sigma_i^p$, $L \in \Pi_i^p \subseteq \Sigma_i^p$. Thus $L \in \Pi_i^p$.

This shows that $\Sigma_i^p = \Pi_i^p$.

\[\square\]