Problem 1

\textit{Proof.} Note that $\Pi_i^p = \text{co} \Sigma_i^p$. Suppose $\Pi_i^p \subseteq \Sigma_i^p$, then for any language $L \in \Sigma_i^p$, $\overline{L} \in \Pi_i^p \subseteq \Sigma_i^p$. Thus $L \in \Pi_i^p$. This shows that $\Sigma_i^p \subseteq \Pi_i^p$. Hence $\Sigma_i^p = \Pi_i^p$. The case of $\Sigma_i^p \subseteq \Pi_i^p$ is completely symmetric.

\hfill \Box

Problem 2

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

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

Assume $\Sigma_j^p = \Sigma_i^p$ for some integer $j > i$, 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

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

(1)

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

Define the language $L'$ as follows:

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

Thus

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

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

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

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

This means

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

By combining $\exists u_1 \in \{0,1\}^{q(|x|)}$ and $\exists u_2 \in \{0,1\}^{q'(|x|)}$ into $\exists (u_1, u_2) \in \{0,1\}^{q(|x|)+q'(|x|)}$, 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 $L \in \Sigma_i^p$ (since $\Pi_i^p \subseteq \Sigma_i^p$). As $\Sigma_i^p \subseteq \text{PH} = \Sigma_i^p$, $L \in \Sigma_i^p$.

By problem 1, this shows that $\Sigma_i^p = \Pi_i^p$.

\hfill \Box

Problem 3

\textit{Proof.} The idea is to construct a specific circuit for every possible length $n$, as in the proof that $P_{/\text{poly}}$ contains undecidable languages. Specifically, fix a particular length $n$, let $S_n = L \cap \{0,1\}^n$ and $|S_n| = t_n$.

We can construct a circuit $C_n$ that accepts every string in $S_n$ and rejects every string outside of $S_n$. The circuit is simply $\bigvee_{i=1}^{t_n} (x = S_i^n)$ where $S_i^n$ is the $i$'th string in $S_n$. The function $(x = S_i^n)$ can be expressed by a linear size AND as we have seen before. Since $t_n \leq p(n)$ for some polynomial $p$, the combined circuit still has polynomial size.

\hfill \Box
Problem 4

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

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

(2)

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, $Pr_{A,b}[Ax + b = y \land Ax' + b = y'] = 1/2^k$. So $H_{A,b}$ is a pairwise independent hash function family.

Problem 5

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 prover can just send that reply. Let these strings form the set $A \subseteq \{0, 1\}^n$. Thus $|A| \geq 2^{n/3}$.

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.