1. The class MA is analogous to NP where the verifier can be a randomized algorithm. There is an all powerful prover (called Merlin) who gives a proof to the probabilistic polynomial time verifier (called Arthur). Arthur uses a (private) random string $r$.

Define the class of languages $\text{MA}_{2/3,1/3}$ with two sided error as follows.

$$x \in L \Rightarrow \exists y, \Pr_r[V(x, y, r) = 1] \geq \frac{2}{3}$$

$$x \notin L \Rightarrow \forall y, \Pr_r[V(x, y, r) = 1] \leq \frac{1}{3}$$

Here $V(\cdot, \cdot)$ is a deterministic polynomial time verification procedure and lengths of $y$ are $r$ are polynomially bounded in the length of $x$.

Similarly we define the class $\text{MA}_{1,1/3}$ with one-sided error as follows.

$$x \in L \Rightarrow \exists y, \Pr_r[V(x, y, r) = 1] = 1$$

$$x \notin L \Rightarrow \forall y, \Pr_r[V(x, y, r) = 1] \leq \frac{1}{3}$$

Show that $\text{MA}_{2/3,1/3} = \text{MA}_{1,1/3}$. That is, if a language has a MA-protocol with two-sided error, then it also has a MA-protocol with one-sided error. \textit{Hint: Use ideas from the proof of BPP $\subseteq \Sigma_2$.}

2. Show that

$$\text{PSPACE} \subseteq \text{P/poly} \Rightarrow \text{PSPACE} = \Sigma_2$$

\textit{Hint: Modify the proof of Karp-Lipton Theorem for a self reducible PSPACE complete problem.}
3. In this question all circuit classes are non-uniform. Show that for any non-negative integer \( i \),

\[ NC^i = NC^{i+1} \Rightarrow NC = NC^i \]

4. Assume that the problem of counting the number of matchings (not just perfect matchings) in a graph is \#P-complete. Show that the problem of counting the number of satisfying assignments to an instance of 2-SAT is \#P-complete.

5. Pairwise Independent Hash Functions
Consider the following family of functions \( F \) that map \( \{0,1\}^n \to \{0,1\}^k \). Pick a \( k \times n \) matrix \( A \) with 0,1 entries at random. Pick \( b \in \{0,1\}^k \) at random. Let

\[ f(x) = Ax + b \]

where all arithmetic operations are over \( \mathbb{Z}_2 \). Assume that \( f \in F \) is picked uniformly at random (by choosing \( A \) and \( b \) randomly).

- Show that for any \( x \in \{0,1\}^n \) and \( y \in \{0,1\}^k \),

\[ \Pr_{A,b}[f(x) = y] = \frac{1}{2^k} \]

*Hint: first consider the case when \( k = 1 \)*

- Show that for any \( x_1, x_2 \in \{0,1\}^n \) and \( x_1 \neq x_2 \), and any \( y_1, y_2 \in \{0,1\}^k \),

\[ \Pr_{A,b}[(f(x_1) = y_1) \land (f(x_2) = y_2)] = \frac{1}{2^{2k}} \]

- Show that for any \( x_1, x_2 \in \{0,1\}^n \) and \( x_1 \neq x_2 \),

\[ \Pr_{A,b}[f(x_1) = f(x_2)] = \frac{1}{2^k} \]

6. We will use pairwise independent hash functions to design an AM protocol for MANY-SAT. The problem is that we are given a SAT instance \( \phi \) with \( S \) as the set of its satisfying assignments. We are told that either \( |S| \geq 2^k \) (YES case) or \( |S| \leq 2^{k-10} \) (NO case). We have to distinguish the YES and NO cases.

Consider the following AM protocol for MANY-SAT. Arthur picks a
random hash function $f_{A,b} : \{0,1\}^n \rightarrow \{0,1\}^k$, and a random target value $y \in \{0,1\}^k$. Merlin sends $x \in \{0,1\}^n$ as answer. Arthur accepts iff $f_{A,b}(x) = y$ and $x$ is a satisfying assignment to $\phi$.

Show that this is a valid AM protocol i.e the probability of acceptance in the YES case is significantly larger than the NO case.

*Hint:* In the YES case, show that there are not too many collisions, the size of the image of $S$, i.e. $|f_{A,b}(S)|$ is likely to be large, and a random $y \in \{0,1\}^k$ is likely to have a pre-image.