Definition 1 Recall that AM[f] for a proper function f denotes the class of languages L such that for any ℓ ≥ 0, there exists a game of Arthur and Merlin (M, A, D) such that for any x of size n, letting prot = (AM)f(n):

1. Completeness: if x ∈ L then prot[A, M]D = ⊤ with probability at least 1 − 1/2^{n^ℓ}
2. Soundness: if x /∈ L then for any Merlin’s function M’, prot[A, M’]D = ⊥ with probability at least 1 − 1/2^{n^ℓ}

Exercise 1: Arthur-Merlin protocols
Prove the following statements, directly from definition of Arthur-Merlin games:

• M = NP;
• A = BPP;
• NP^{BPP} ⊆ MA;
• AM ⊆ BPP^{NP}.

Exercise 2: Collapse of the Arthur-Merlin hierarchy
Recall that, for each Π ∈ {A, M}*, the class Π is the class of languages recognized by Arthur-Merlin games with protocol Π.

(a) Without using any result about the collapse of the Arthur-Merlin hierarchy, prove that for all Π₀, Π₁, Π₂ ∈ {A, M}*, we have Π₁ ⊆ Π₀Π₁Π₂.

(b) Now assume the fact that for all Π ∈ {A, M}* , one has Π ⊆ AM. Prove the following statement: For all Π ∈ {A, M}* such that Π has a strict alternation of symbols, and |Π| > 2, we have Π = AM.

Exercise 3: The BP operator
We say that a language B reduces to language C under a randomized polynomial time reduction, denoted B ≤^r_r C, if there is a probabilistic polynomial-time Turing machine such that for every x, Pr[C(M(x)) = B(x)] ≥ 2/3.

1. Show that BP · C = {L | L ≤^r_r L’, for some L’ ∈ C}
2. Show that BPP is closed under randomized polynomial time reduction.
3. Deduce that BP · (BP · C) = BP · C.
Exercise 4: The class $\text{BP} \cdot \text{NP}$

1. Show that $\text{BP} \cdot \text{P} = \text{BPP}$
2. Show that $\text{BP} \cdot \text{NP} = \text{AM}$
3. Show that $\text{BP} \cdot \text{NP} \subseteq \text{NP/poly}$
4. Show that $\text{BP} \cdot \text{NP} \subseteq \Sigma^P_3$ (give a direct proof, do not use $\text{AM} \subseteq \Pi^P_2$).
5. Show that if $3\text{SAT} \leq_r 3\text{SAT}$ then $\text{PH}$ collapses to the third level.

Exercise 5: One Merlin to rule them all

Show that the following definition of $\text{AM}$ if actually equivalent to the one given in introduction: $L \in \text{AM}$ if for any $\ell \geq 0$, there exists an Arthur $A$ and a polynomial-time-checkable predicate $D$ such that for any $x$ of size $n$, letting $\text{prot} = (\text{AM})^{f(n)}$:

1. Completeness: if $x \in L$ then there exists some Merlin $M$ such that $\text{prot}[A, M]|_D = \top$ with probability at least $1 - 1/2^{n^{\ell}}$
2. Soundness: if $x \notin L$ then for any Merlin $M'$, $\text{prot}[A, M']|_D = \bot$ with probability at least $1 - 1/2^{n^{\ell}}$

Exercise 6: Unreliable Merlin

Show that allowing Merlin to use randomness (in a private manner) does not change the class $\text{AM}$.