Exercise 1.

**Definition** (Zero-error Probabilistic Polynomial time). The class ZPP is defined as the set of languages $L$ such that there exists a polynomial $p$ and a TM $M$ with three halting states $q_{\text{accept}}, q_{\text{reject}}$ and $q_{\text{meh}}$, such that on every input $x \in \Sigma^*$ we have:

- $\Pr_{r \in \{0,1\}^{|x|}} [M(x, r) \rightarrow q_{\text{reject}} | x \in L] = 0$ and $\Pr_{r \in \{0,1\}^{|x|}} [M(x, r) \rightarrow q_{\text{meh}} | x \in L] \leq 1/2$
- $\Pr_{r \in \{0,1\}^{|x|}} [M(x, r) \rightarrow q_{\text{accept}} | x \notin L] = 0$ and $\Pr_{r \in \{0,1\}^{|x|}} [M(x, r) \rightarrow q_{\text{meh}} | x \notin L] \leq 1/2$

In other words, $M$ will never answer incorrectly, but can return « I don’t know » (state $q_{\text{meh}}$) with probability $\leq \frac{1}{2}$.

1. Show that $\text{ZPP} = \text{RP} \cap \text{coRP}$.
2. Recall how to reduce the error to recognize a language in $\text{RP}$.
3. Prove that $L \in \text{ZPP}$ iff there exists a probabilistic Turing machine $M$ that recognizes $L$ with probability $1$, and whose expected running time is polynomial.

Exercise 2.

**Definition** (Schwarz-Zippel Lemma). Let $F$ be a field. If a polynomial $P = \sum_{i=0}^{\ell} \prod_{j=1}^{n} X_i^{v_{ij}} \in F[X_1, \ldots, X_n]$ has total degree $d = \max_j \sum_{i=1}^{n} v_{ij}$. Let $S \subseteq F$ and $r_1, \ldots, r_n \leftarrow U(S)$ independently, then

$$\Pr[P(r_1, \ldots, r_n) = 0] \leq \frac{d}{|S|}$$

1. Prove the Schwarz-Zippel Lemma.
2. Deduce a randomized algorithm to test if a polynomial is zero, for an infinite field. Bound its error probability.
3. In the case where the polynomial may be *sparse*, it is represented as an algebraic circuit — with variables in the leaves, and operations $+, -, \times$. Supposing the circuit has size $m$, bound its degree, and give an estimate of the expected arithmetic cost (in terms of operations in $F$) of deciding if it is zero.

Exercise 3.

NP/poly A nondeterministic circuit has two inputs $x, y$. We say that $C$ accepts $x$ if and only if there exists $y$ such that $C(x, y) = 1$. The size of the circuit is measured as a function of $|x|$.

Let NP/poly be the languages that are decided by polynomial size nondeterministic circuits.

BP · NP is defined as the class of language $A$ such that there exists a polynomial $p$ and a language $B \in \text{NP}$ such that, for every word $x$:

$$\begin{cases} x \in A \implies \Pr_{r \in \{0,1\}^{|x|}} ((x, r) \in B) \geq 2/3 \\ x \notin A \implies \Pr_{r \in \{0,1\}^{|x|}} ((x, r) \notin B) \geq 2/3 \end{cases}$$

1. Show that $\text{BP} \cdot \text{NP} \subseteq \text{NP/poly}$.
**Definition (AM).** The class AM (Arthur-Merlin) is defined as the class of decision problems such that it can be verified by an *Arthur-Merlin protocol* defined as follows: Arthur, a BPP verifier, generates a challenge $c$ based on the input, and sends it together with its random coin to Merlin. Then Merlin sends back an answer, and Arthur chooses if it accepts or not.

Given an algorithm “Arthur”, it is required that

- If the input is in the language, then Merlin can act in such a way that Arthur accepts with probability at least $\frac{2}{3}$ (over the choice of Arthur’s random bits).
- Otherwise, then however Merlin acts, Arthur will reject with probability at least $\frac{2}{3}$.

2. Show that $\text{BP} \cdot \text{NP} = \text{AM}$.

**Exercise 4.**

**Biased Definition.** A $\rho$-coin, is a biased coin such that $\Pr[\text{HEAD}] = \rho$.

1. Show that a $\rho$-coin can be simulated by a probabilistic Turing machine (PTM) in expected running time $O(1)$ if the $i$-th bit of $\rho$ can be computed in $\text{poly}(i)$.

2. (Von Neumann) Conversely, show that a $\frac{1}{2}$-coin can be simulated by a $\rho$-coin in expected running time $O\left(\frac{1}{\rho(1-\rho)}\right)$.

3. Propose a method to improve the running time expectation of the latest machine.

4. Propose a real number $\rho$ such that a PTM with an access to a $\rho$-coin can decide an undecidable language.