Tutorial 12 – Probably the last one

Exercise 1. *Let us have fun with definitions...*

1. Show that in the definition of BPP, the constant $2/3$ can be replaced by $f(|x|)$ where f is any function verifying $1/2 + n^{-c} \leq f(n) \leq 1 - 2^{-n^d}$ with $c, d > 0$.
2. Do those bounds still hold in the case of RP?
3. Show that the following three definitions are equivalent:
   1. ZPP is the class of languages s.t. there exists a polytime PTM which gives than right answer with probability at most $1/2$, and answers "I don't know" otherwise;
   2. ZPP is the class of languages s.t. there exists a PTM which always gives the right answer and which stops in expected polynomial time;
   3. $\mathsf{ZPP} = \mathsf{RP} \cap \mathsf{coRP}$.
4. Show that $\mathsf{RP} \subseteq \mathsf{NP}$.
5. And $\mathsf{RP} \subseteq \mathsf{P/poly}$?

Exercise 2.
A ρ-coin is a biased coin s.t. $\mathbb{P}[\textsc{Face}] = \rho$.

1. Show that a ρ-coin can be simulated by a PTM in expected time $O(1)$ if the i-th bit of ρ is computable in time $\mathsf{poly}(i)$.
2. (Von Neumann's method) Conversely, show that a $1/2$-coin can be simulated by a ρ-coin in expected time $O(1/\rho(1-\rho))$.
3. Propose a method to improve the expected time.
4. Give a real number ρ s.t. a PTM using a ρ-coin can decide an undecidable language.
5. Show taht a uniform sampling in $\{1, \dots, N\}$ can be simulated with a coin: For all N and $\delta > 0$, there exists a probablistic algorithm A, working in time $\mathsf{poly}(\log(N)\log(1/\delta))$, which outputs an element from $\{1, \dots, N, ?\}$ s.t.
   1. if it does not output ?, the output $\{1, \dots, N\}$;
   2. The probability that A outputs ? is at most δ.

Exercise 3. *Let's draw!*
Justify everything: