17. For constants $0 < \alpha < \beta < 1$, define the class $\text{BPP}_{\alpha, \beta}$ to be the class of all languages $A \subseteq \Sigma^*$ such that there exists a PTM $M$ that runs in polynomial time and behaves as follows on an input $x \in \Sigma^*$:

$$
x \notin A \Rightarrow \Pr_R[M(x, r) = 1] \leq \alpha,
$$

$$
x \in A \Rightarrow \Pr_R[M(x, r) = 1] \geq \beta.
$$

Note that our definition of $\text{BPP}$ in class coincides with $\text{BPP}_{\frac{1}{2}, \frac{3}{4}}$ in this notation.

Using Chernoff bounds, give a full formal proof that for all $\alpha$ and $\beta$ as above, $\text{BPP}_{\alpha, \beta} = \text{BPP}$. \hspace{1cm} [2 points]

The Chernoff bound has the following general form. Let $\{X_1, \ldots, X_n\}$ be independent indicator random variables with $\mathbb{E}[X_i] = p_i$. Suppose $X = \sum_{i=1}^n X_i$ and let $p$ be such that $np = p_1 + \cdots + p_n$. Then, for any $\delta > 0$:

$$
\Pr[X \geq (1 + \delta)np] \leq \left( \frac{e^\delta}{(1 + \delta)^{1+\delta}} \right)^{np}.
$$

We also have a similar inequality bounding deviations of $X$ below its mean. For $0 < \delta < 1$:

$$
\Pr[X \leq (1 - \delta)np] \leq \left( \frac{e^{-\delta}}{(1 - \delta)^{1-\delta}} \right)^{np}.
$$

These inequalities can be weakened to more convenient forms by using Taylor series expansions of $\ln(1 \pm \delta)$. The Appendix of [Arora-Barak] has more on Chernoff bounds.

18. Prove that $\text{NP} \subseteq \text{BPP}$ implies $\text{NP} = \text{RP}$.

Hint: Once you “solve” one NP-complete problem, you can solve them all! \hspace{1cm} [2 points]

19. (This is a standard exercise in many textbooks; please avoid looking in them for solutions and try to work this out by yourself. It will pay off well later in the course.)

Let $X$ and $Y$ be finite sets and let $Y^X$ denote the set of all functions from $X$ to $Y$. We will think of these functions as “hash” functions.* A family $\mathcal{H} \subseteq Y^X$ is said to be 2-universal if the following property holds, with $h \in_R \mathcal{H}$ picked uniformly at random:

$$
\forall x, x' \in X \ \forall y, y' \in Y \left( x \neq x' \Rightarrow \Pr_{h \in_R \mathcal{H}}[h(x) = y \land h(x') = y'] = \frac{1}{|Y|^2} \right).
$$

Consider the sets $X = \{0, 1\}^n$ and $Y = \{0, 1\}^k$, with $k \leq n$. Treat the elements of $X$ and $Y$ as column vectors with 0/1 entries. For a matrix $A \in \{0, 1\}^{k \times n}$ and vector $b \in \{0, 1\}^k$, define the function $h_{A, b} : X \rightarrow Y$ as follows: $h_{A, b}(x) = Ax + b$, where all additions and multiplications are performed mod 2.

Now consider the family of functions $\mathcal{H} = \{h_{A, b} : A \in \{0, 1\}^{k \times n}, b \in \{0, 1\}^k\}$. Prove that

$$
\forall x \in X \ \forall y \in Y \left( \Pr_{h \in_R \mathcal{H}}[h(x) = y] = \frac{1}{|Y|} \right).
$$

Next, prove that $\mathcal{H}$ is a 2-universal family of hash functions. \hspace{1cm} [2 points]

---

*The term “hash function” has no formal meaning; instead, one should speak of a “family of hash functions” or a “hash family” as we do here.