17. Prove that $\mathsf{NP} \subseteq \mathsf{BPP}$ implies $\mathsf{NP} = \mathsf{RP}$.
   
   Hint: Once you “solve” one $\mathsf{NP}$-complete problem, you can solve them all! [2 points]

18. 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 $h \in \mathcal{H}$ picked uniformly at random:

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

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 $h_{A,b} : X \to Y$ 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

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

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

Note 1: For the last problem, you must solve both parts to receive credit.

Note 2: If you have correctly solved the last problem in a previous course (e.g., the Data Stream Algorithms course), you may hand in your previous solution. This will not be an Honor Code violation.

---

*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.