Problems:

1. Prove that if $\text{NP} \subseteq \text{BPP}$ then $\text{NP} = \text{RP}$.

2. The Vapnik-Chervonenkis (VC) dimension is an important concept in machine learning. If $\mathcal{F} = \{S_1, \ldots, S_m\}$ is a family of subsets of a finite set $U$, the VC dimension of $\mathcal{F}$, denoted $\text{VC}(\mathcal{F})$, is the size of the largest set $A \subseteq U$ such that for every $A' \subseteq A$, there is an $i$ for which $S_i \cap A = A'$. (One says that $A$ is shattered by $\mathcal{F}$.)

A Boolean circuit $C$ with two inputs $i \in \{0, 1\}^r$ and $x \in \{0, 1\}^n$ represents the collection $\mathcal{F} = \{S_1, S_2, \ldots, S_{2^r}\}$ over universe $U = \{0, 1\}^n$ given by $S_i = \{x \in U \mid C(i, x) = 1\}$.

Define the language $\text{VCDIM} = \{[C, 1^k] \mid \text{the collection } \mathcal{F} \text{ represented by } C \text{ has } \text{VC}(\mathcal{F}) \geq k\}$.

Prove that $\text{VCDIM} \in \Sigma^p_3$.

3. Prove that if $A \in \text{BPP}$ then there exists a polynomial-time Turing machine $M$ and a polynomial bound $p$ such that the following property:

- If $x \in A$ then $\exists y \in \{0, 1\}^{p(|x|)} \forall z \in \{0, 1\}^{p(|x|)} (M(x, y, z) = 1)$.
- If $x \notin A$ then $\exists z \in \{0, 1\}^{p(|x|)} \forall y \in \{0, 1\}^{p(|x|)} (M(x, y, z) = 0)$.

In what way is this a stronger inclusion than $\text{BPP} \subseteq \Sigma^p_2 \cap \Pi^p_2$?

(Hint: Extend the approach to proving $\text{BPP} \subseteq \Sigma^p_2$.)

4. We covered two different methods for obtaining lower bounds for deterministic communication complexity. One was via fooling sets: Recall that $F = \{(x_1, y_1), \ldots, (x_m, y_m)\}$ is a 1-fooling set for $f$ iff for all $i \neq j$, $f(x_i, y_i) = 1$ but either $f(x_i, y_j)$ or $f(x_j, y_i)$ equals 0. Then $D^{cc}(f) \geq \log_2 |F|$. We also showed that $D^{cc}(f) \geq \log_2 \text{rank}(M_f)$.

Show that for any 1-fooling set $F$, $|F| \leq \text{rank}(M_f)^2$ and therefore the rank lower bound is at least half the 1-fooling set lower bound. To do this define a new matrix $M^*$ which is the outer product $M_f \otimes M_f^T$ and look at the submatrix of $M^*$ whose row and columns are indexed by elements of $F$.

(Given matrices $A$ and $B$, matrix $A \otimes B$ is the matrix with $\text{rows}(A) \cdot \text{rows}(B)$ rows and $\text{cols}(A) \cdot \text{cols}(B)$ columns that replaces each entry $a_{ij}$ of $A$ with the matrix $a_{ij}B$. You will need the fact that $\text{rank}(A \oplus B) = \text{rank}(A) \cdot \text{rank}(B)$.)
5. (Extra credit) Show that $VCDIM$ is complete for $\Sigma_3^p$.

6. (Extra credit) Reingold proved that $UPATH \in L$. The proof involves construction of certain expander graphs and an interesting iterative improvement argument. Instead of using that result or its proof, give a logspace algorithm that determines $UCYCLE$, whether or not an undirected graph $G$ contains a cycle.