Problem 1

(10 pts.) Prove that for every AM[2] protocol for a language $L$, if the prover and the verifier repeat the protocol $k$ times in parallel (verifier runs $k$ independent random strings for each message) and the verifier accepts if all $k$ copies accept, then the probability that the verifier accepts $x \notin L$ is at most $(1/3)^k$. Note that you cannot assume that the prover is acting independently in each execution. (Use definition 8.6 for IP from Arora Barak).

Problem 2

(10 pts.) Define a language $L$ to be downward-self-reducible if there is a polynomial time algorithm $R$ that for any $n$ and $x \in \{0,1\}^n$, $R^{L_n-1}(x) = L(x)$ where by $L_k$ we denote an oracle that solves $L$ on inputs of size at most $k$. Prove that if $L$ is downward-self-reducible then $L \in \text{PSPACE}$.

Problem 3

Recall that the trace of a matrix $A$, denoted $tr(A)$ is the sum of the entries along its diagonal.

- (5 pts.) Prove that if an $n \times n$ matrix $A$ has eigenvalues $\lambda_1, \ldots, \lambda_n$, then $tr(A) = \sum_{i=1}^{n} \lambda_i$.

- (5 pts.) Prove that if $A$ is a random walk matrix of an $n$-vertex graph $G$ and $k \geq 1$, then $tr(A^k)$ is equal to $n$ times the probability that if we select a vertex $i$ uniformly at random and take a $k$ step random walk from $i$, then we end up back in $i$.

- (5 pts.) Prove that for every $d$-regular graph $G$, $k \in \mathbb{N}$ and vertex $i$ of $G$, the probability that a path of length $k$ from $i$ ends up back in $i$ is at least as large as the corresponding probability in $T_d$, where $T_d$ is the complete $(d-1)$-ary tree
of depth \( k \) rooted at \( i \). (that is, every internal vertex has degree \( d \), one parent and \( d - 1 \) children.)

- (5 pts.) Prove that for even \( k \), the probability that a path of length \( k \) from the root of \( T_d \) ends up back at \( v \) is at least \( 2^{k - k \log(d - 1)/2 + o(k)} \).

**Problem 4**

(20 pts.) Show that it is impossible to make constant-degree expander Cayley graphs from abelian groups.

**Problem 5**

- (10 pts.) Prove that \( PCP(0, \log n) = P \). Prove that \( PCP(0, \text{poly}(n)) = NP \).
- (10 pts.) Show the following equivalent characterization of \( NP \):
  \( NP = \{ L : \text{there is a logspace machine } M \text{ s.t. } x \in L \text{ iff } \exists y : \text{M accepts } (x, y) \} \).
  Where \( M \) has two-way access to \( y \), meaning that \( M \) can move its head back and forth on the certificate.
- (20 pts.) Let \( L-PCP(r(n)) \) be the class of languages whose membership proofs can be probabilistically checked by a logspace machine that uses \( O(r(n)) \) random bits but makes only one pass over the proof. (It has two-way access to \( x \) but one-way access to \( y \)). The completeness and soundness parameters are 1 and \( 1/2 \) respectively. Without assuming the PCP theorem, show that \( NP = L-PCP(\log n) \).

**Problem 6**

(10 pts.) Consider the following problem: Given a system of linear equations in \( n \) with coefficients that are rational numbers, determine the largest subset of equations that are simultaneously satisfiable over the rationals. Show that there is a constant \( \rho < 1 \) such that approximating the size of this subset is \( NP \)-hard.