Answer all five of the following questions. Please remember to write your name, CPSC 468/568, and today’s date on the covers of all blue books you submit.

Question 1

Recall that the permanent of an n-by-n, integer-valued matrix A is defined by the formula

$$\text{Perm}(A) = \sum_{\sigma} \prod_{i=1}^{n} A_{i \sigma(i)} \quad (*)$$

(a) (10 points) For general integer matrices, give an alternative definition of the permanent in terms of cycle covers, and prove that this definition is equivalent to (*).

(d) (10 points) Consider the directed graph below. Prove that the permanent of the matrix corresponding to this digraph is 0.

![Directed graph with arrows and numbers]

Question 2

Recall Definition 8.6 of a k-round interactive proof system for the language L (where k may be a function of the length n of the input string x): There is a probabilistic, polynomial-time verifier V that can have a k-round interaction with a prover Q: \{0, 1\}^* \rightarrow \{0, 1\}^* such that, if x is in L, then there exists a P such that Prob((V,P)(x) = 1) ≥ 2/3, and, if x is not in L, then, for all P*, Prob((V,P*)(x) = 1) ≤ 1/3. (Here “(V,Q)(x)” denotes the output of V after k rounds of interaction with Q. The probabilities are computed over the coin tosses of V.)

This question focuses on variations on the basic Definition 8.6 and their computational power.

(a) (6 points) What is a k-round public-coin interactive proof system (aka a k-round Arthur-Merlin proof system)?

(b) (8 points) Give a short explanation of why polynomial-round public-coin interactive proof systems are as powerful as the unrestricted polynomial-round interactive proof systems of Definition 8.6.

(c) (6 points) What is a k-round program checker?
Question 3
(a) (10 points) Let $S \subseteq \{0, 1\}^m$ be a set in which membership can be quickly certified. (Here “certified” is used in the NP sense: There is a polynomial $p$ and a polynomial-time Turing Machine $M$ such that $x$ is in $S$ if and only if there is a $w$ in $\{0, 1\}^{p(m)}$ such that $M(x, w) = 1$; $w$ is a “certificate” of $x$’s membership in $S$.) Give a protocol that a prover $P$ can use to convince a verifier $V$ that $|S|$ is at least $K$, where $K$ is an integer known to both $P$ and $V$. The protocol should succeed (i.e., cause $V$ to accept) whenever $|S| \geq K$ and should fail (i.e., cause $V$ to reject) whenever $|S| \leq K/2$; there is no requirement on what should happen if $K/2 < |S| < K$. (Just state the protocol; you need not prove that it has this property.)

(b) (10 points) Let $L$ be a language in BPP and $M$ be a machine that recognizes $L$ with exponentially small error probability; that is, for all $n$ and all $x$ in $\{0, 1\}^n$, if $x$ is in $L$, then $M(x, s) = 1$ for at least $(1-2^{-n})2^m$ of the strings $s$ in $\{0, 1\}^m$, and, if $x$ is not in $L$, then $M(x, s) = 1$ for at most $2^{-n}2^m$ of the strings $s$ in $\{0, 1\}^m$. (Here $m$ is a polynomially bounded function of $n$.)

As in the proof of the Sipser-Gacs Theorem, let $V = \{0, 1\}^m$ and $k = 1 + (m/n)$, and consider, for $U = \{u_1, \ldots, u_k\} \subseteq V$, the undirected graph $G_U = (V, E)$, where the edge $(r, s)$ is in $E$ if and only if $r = s \oplus u_i$ (the bitwise exclusive-or of $s$ and $u_i$). $\Gamma_U(S)$ denotes the neighborhood of the set $S$, i.e., the set of all $r$ in $V$ such that there is an $s$ in $S$ and a $u_i$ in $U$ for which $r = s \oplus u_i$. Sipser and Gacs use the probabilistic method to show that, if $|S| \leq (2^{-n})2^m$, then there is no $U$ of size $k$ for which $\Gamma_U(S) = \{0, 1\}^m$, and, if $|S| \geq (1-2^{-n})2^m$, then there is a $U$ of size $k$ such that $\Gamma_U(S) = \{0, 1\}^m$.

Use this fact to complete the proof of the Sipser-Gacs Theorem, i.e., to complete the proof that $\text{BPP} \subseteq \sum_2^p \cap \Pi_2^p$.

Question 4
State whether each of the following claims is true, false, or unknown. If you answer true or false, give a very brief justification.
(a) (5 points) $\text{PH} \subseteq \text{BPP}^\oplus_p$

(b) (5 points) $\text{PH} \subseteq \text{P}^\oplus_p$

(c) (5 points) $\text{PH} \subseteq \text{P}^{\oplus_p}$

(d) (5 points) $\text{BPP} = \text{P}/\text{poly}$

Question 5
(a) (8 points) Recall that $\omega(G)$ is the size of the largest clique in $G$ and that, if there is a deterministic polynomial-time algorithm that approximates $\omega(G)$ within a factor of 2, then $\text{EXP} = \text{NEXP}$. Explain briefly why essentially the same proof can be used to prove that, if there is a deterministic polynomial-time algorithm that approximates $\omega(G)$ within a factor of $c$, for any constant $c$, then $\text{EXP} = \text{NEXP}$.
(b) (6 points) Define the complexity classes ZPP and BPP. Prove that one of them is contained in the other.

(c) (6 points) Prove that $\text{BPP} = \text{P}$ if $\text{NP} = \text{P}$. 