Interactive Proofs

Problem 1: Pairwise Independent Hash Functions

Let $H$ be a collection of functions such that $h : X \rightarrow Y$ for each $h \in H$ and let $A$ be a Turing program such that $A(x, h) = h(x)$ and $A$ runs in time polynomial in $|x|$ (where we assume some reasonable bit representation of $x$ and $h$).

We call $H$ a pairwise independent hash function family if for all $x \neq x' \in X, y, y' \in Y$:

$$\Pr_h[h(x) = y \land h(x') = y'] = \frac{1}{|Y|^2},$$

where the choice of $h$ is uniform over $H$.

a) Let us interpret bitstrings in $\{0, 1\}^n$ as elements of the field $\mathbb{F}_2^n$. Show that $\{h_\alpha, \beta\}_{\alpha, \beta} \in \mathbb{F}_2^n$ with $h_\alpha, \beta : \{0, 1\}^n \rightarrow \{0, 1\}^n$ and $h_\alpha, \beta(x) = \alpha \cdot x + \beta$ is a pairwise independent hash function family. You can assume without proof that $h_\alpha, \beta$ are efficiently computable.

b) Use a) to argue that for every $n, k \in \mathbb{N}$ there exists a pairwise independent hash function family $H$ with $H \ni h : \{0, 1\}^n \rightarrow \{0, 1\}^k$.

c) Let $H$ be a pairwise independent hash function family with $H \ni h : \{0, 1\}^n \rightarrow \{0, 1\}^k$ and let $S \subseteq \{0, 1\}^n$.

\begin{itemize}
  \item If $|S| \geq 2^k$, then $\Pr_h[h^{-1}(0^k) \cap S \neq \emptyset] \geq \frac{1}{2}$.
  \item If $|S| \leq \frac{2^k}{c}$ for $c > 2$, then $\Pr_h[h^{-1}(0^k) \cap S \neq \emptyset] \leq \frac{1}{c}$.
\end{itemize}

d) Let the setting be as in c). Prove the following hash mixing lemma:

$$\Pr_h\left[\left|\left|h^{-1}(0^k) \cap S\right| - \frac{|S|}{2^k}\right| \geq \frac{c|S|}{2^k}\right] \leq \frac{2^k}{c^2|S|}.$$

Problem 2: Public-Coin Protocol for Graph Non-isomorphism

Let $G = (V, E)$ be a simple graph, where we identify $G$ with its adjacency matrix. Let $n := |V(G)|$.

We denote by $S_n$ the set of all permutations on $[n]$. Furthermore, we identify $\pi \in S_n$ with a corresponding permutation of the adjacency matrix of $G$. This should lead to no confusion.

Let $\text{Aut}(G) := \{\pi \in S_n : \pi(G) = G\}$. We call $\pi \in \text{Aut}(G)$ an automorphism of $G$.

a) Let $P_G := \{(\pi(G), \sigma) \mid \pi \in S_n, \sigma \in \text{Aut}(\pi(G))\}$. Show that $|P_G| = n!$.

b) Use the previous item and c) or d) from the previous exercise to devise a two-round public-coin protocol for graph non-isomorphism.
Problem 3: Private-to-Public-Coin for Two Rounds

Recall that $\text{IP}[2]$ is the class of languages with (private-coin) two-round interactive proofs where the verifier sends the first message. Our goal is to show that $\text{IP}[2] \subseteq \text{AM}$.

Let $L \in \text{IP}[2]$ and $V$ be a verifier with completeness $\frac{2}{3}$ and soundness $2^{-3|x|}$ (this can be achieved by parallel repetition, hopefully the proof is clear).

Let $V$ sample randomness $r$, then send a message $m$ and receive a witness $w$ from the prover. Moreover, assume w.l.o.g. that all $r$, $m$ and $w$ have lengths $n^c$ where $n := |x|$.

a) Let $x \in L$ and $m$ be a verifier message. Define

$$r_m := \max_w \left| \{ r : V(r) = m \wedge V(r, m, w) \text{ accepts} \} \right| .$$

Argue that there exists $b \in [n^c]$ such that

$$\left| \{ m : r_m \geq 2^{n^c-b} \} \right| \geq \frac{2^b}{4n^c} .$$

b) Consider the following protocol:

1. Merlin sends $b \in [n^c]$ to Arthur.
2. Arthur computes $k$ such that $2^k \leq \left\lceil \frac{2^b}{4n^c} \right\rceil \leq 2^{k+1}$ and sends a uniform $h_1 \in \mathcal{H}_1$, where $\mathcal{H}_1$ is a pairwise independent family that hashes $\{0,1\}^{n^c}$ to $\{0,1\}^k$. 
3. Merlin responds with a pair $(m, w)$.
4. Arthur sends a uniform $h_2 \in \mathcal{H}_2$, where $\mathcal{H}_2$ is a pairwise independent family that hashes $\{0,1\}^{n^c}$ to $\{0,1\}^{n^c-b}$.
5. Merlin responds with $r$.
6. Arthur checks if $h_1(m) = 0^k$ and $h_2(r) = 0^{n^c-b}$. Then, he checks if $V(r) = m$ and $V(r, m, w)$ accepts. He accepts iff all the checks succeeded.

Use the protocol above to show that $\text{IP}[2] \subseteq \text{AM}$. 