Homework 13

Problem 1. Prove that for every AM protocol for a language A, if Merlin and Arthur repeat the protocol k times in parallel (Arthur runs k independent random strings for each message and accepts only if all k copies accept), then the probability that Arthur accepts $x \notin A$ is at most $1/2^k$. (Recall that an AM protocol starts with Arthur sending the random string and Merlin replying a witness. You should not assume that the Merlin message for parallelized protocol is independent for each copy in your proof.)

Solution. In the k parallel repetition of the AM protocol, Arthur would send message $R = (r_1, r_2, \ldots, r_k)$ to Merlin, and Merlin would respond $(m_1, m_2, \ldots, m_k)$ to Arthur. The major difficulty in the proof is that now for each message m_i, it might depend on the full R, making it hard to claim any 'independent' style claims.

Let us use V_i as the ith parallel Arthur's algorithm. We have the following observation, for any $x \notin L$, given any fixed $r_1^*, r_2^*, \ldots r_{i-1}^*$,

$$\Pr_{R=(r_1^*,\ldots,r_{i-1}^*,r_i,\ldots,r_k)}[V_i(x, r_i, m_i(R)) = 1] \leq \frac{1}{2}.$$

This step is by the soundness guarantee of the original AM protocol. Given the malicious Merlin P^* in the parallel repeated protocol, we construct a P_i^* as follows: It hardcodes $r_1^*, r_2^*, \ldots r_{i-1}^*$ in its program, and samples $r_{i+1}, r_{i+2}, \ldots, r_k$ by itself. After receiving r_i from Arthur, it sends R to P^*, and reply Arthur with message $m_i(R)$, giving us the above bound by the soundness guarantee.

Moreover, this step implies the following result for $i = 1, \ldots, k$:

$$\Pr_R\left[V_i(x, r_i, m_i(R)) = 1 \,\middle|\, \bigwedge_{j=1}^{i-1} V_j(x, r_j, m_j(R)) = 1\right] \leq \frac{1}{2}.$$

By the conditional probability formula, we have that

$$\Pr\left[\bigwedge_{i=1}^{k} V_j(x, r_i, m_i(R)) = 1\right] = \prod_{i=1}^{k} \Pr_R\left[V_i(x, r_i, m_i(R)) = 1 \,\middle|\, \bigwedge_{j=1}^{i-1} V_j(x, r_j, m_j(R)) = 1\right] \leq \frac{1}{2^k}$$

Problem 2.

(a) Explain why the following simulator does not work in establishing the zero-knowledge property of the protocol for GRAPH-ISO discussed in the class.

1: Choose $a \in \{0, 1\}$ uniformly at random.
2: Sample a random permutation π and compute $G = \pi(G_a)$.
3: Randomly sample $b \in \{0, 1\}$.
4: If $b = a$, output the transcript. Otherwise, rewind and start from the beginning.

(b) Prove the zero-knowledge property of the protocol for GRAPH-ISO discussed in the class formally.

Solution. (a) The simulator does not work when the verifier is malicious, since a malicious verifier can always send $b^* = 1$, while the simulator will generate view with $b = 0$.

(b) The major step is to prove that the distribution $\{\pi(G_0)\} \equiv \{\pi(G_1)\}$ for the case when G_0 and G_1 are isomorphic. After showing that, we can see conditional on $b = b^*$, the transcript distribution is identical. The two distribution are the same, since there exists a permutation σ s.t. $G_1 = \sigma(G_0)$, and we can see that for any fixed σ, $\{\pi(G_1)\} \equiv \{(\pi \circ \sigma)(G_0)\} \equiv \{\pi(G_0)\}$.

Since b and b^* is independent, we can see that the expected repetition time is 2.