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. The AM protocol satisfies that if $x \notin A$ then $\Pr(\langle P, V\rangle(x) = 1) \leq 1/2$. Consider each time the Verifier generates random string r_i, and denote this simulation as $\langle P, V\rangle_i$. We need to prove that for all $x \notin A$, $\Pr(\bigwedge_{i=1}^{k}\langle P, V\rangle_i(x) = 1) \leq 1/2^k$. Use induction. Assume that $\Pr(\bigwedge_{i=1}^{k-1}\langle P, V\rangle_i(x) = 1) \leq 1/2^{k-1}$, and prove the k case below. If $\Pr(\bigwedge_{i=1}^{k-1}\langle P, V\rangle_i(x) = 1) \leq 1/2^k$, then obviously the conditional probability is not greater than 1, and the proof should be done. Thus, we only need to consider the case when $\Pr(\bigwedge_{i=1}^{k-1}\langle P, V\rangle_i(x) = 1) \geq 1/2^k$. Below we will prove that $\Pr(\langle P, V\rangle_k(x) = 1 | \bigwedge_{i=1}^{k-1}\langle P, V\rangle_i(x) = 1) \leq 1/2$

If $\Pr(\langle P, V\rangle_k(x) = 1 | \bigwedge_{i=1}^{k-1}\langle P, V\rangle_i(x) = 1) > 1/2$ for some $x \notin A$: Because in Merlin-Arthur mode the Verifier has no private information, its every move can be simulated. Consider a P' as follows: On any input random string r_k:

1. Simulate $\langle P, V\rangle_i$ for $i = 1, 2, ..., k-1$.
2. If some simulations reject, rewind from step 1.
3. Until all simulations accpet. we simulate P with the r_i s generated in the last simulation, and the new input r_k.

Now we will prove thie P' can always halt and is correct. If $x \in A$ then al $\langle P, V\rangle_i$ will accept in the first round and then P' will accept. If $x \notin A$, from the induction hypothesis and the further assumption made above, the probability of the $k-1$ $\langle P, V\rangle_i$ all accepting is greater than $1/2^k$, so by continuing simulating step 3 will always be reached. (The probability of P' not halting is 0.)

However, using this P' on the protocol we have $\Pr(\langle P', V\rangle(x) = 1) = \Pr(\langle P, V\rangle_k(x) = 1 | \bigwedge_{i=1}^{k-1}\langle P, V\rangle_i(x) = 1) > 1/2$ where $x \notin A$, which is a contradiction to the property of the AM protocol. Thus we have $\Pr(\langle P, V\rangle_k(x) = 1 | \bigwedge_{i=1}^{k-1}\langle P, V\rangle_i(x) = 1) \leq 1/2$ when $\Pr(\bigwedge_{i=1}^{k-1}\langle P, V\rangle_i(x) = 1) > 1/2^k$. Using the induction hypothesis we have $\Pr(\bigwedge_{i=1}^{k-1}\langle P, V\rangle_i(x) = 1) \leq 1/2^k$. By induction, the proof is done.

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) To establish the ZK property, the simulator needs to have $S(x) = \text{view}_{V^*}\langle P, V^*\rangle(x)$ for all V^* and all $x \in$ GRAPH-ISO. This simulator choose b uniformly at random, but we can construct some V^* to choose b at another distribution. For example, let $\Pr(b = 1) = 0.9$. In S, the probability of the final chosen b is $\Pr(b = 1) = 0.5$ since a and b are both uniformly chosen and the result of 1 and 0 should be symmetric. Thus, the two distribution are distinguishable by b.

(b) We need to prove that distribution $S(x) = \text{view}_{V^*}\langle P, V^*\rangle(x)$ for all V^* and all $x \in$ GRAPH-ISO. For any given $x \in$ GRAPH-ISO and V^*, $\text{view}_{V^*}\langle P, V^*\rangle(x)$ gives uniformly sampled graph G isomorphic to the two graphs, a bit b and a permutation between G and G_b. For S, it gives a uniformly sampled G as well, and gives a b by simulating V^*, and then a permutation. We only need to prove the distribution of b is the same, because the permutation can be uniquely determined by G and b.

Say in V^*, $\Pr(b_{V^*} = 1) = p$. Then in S, Say the sampled a, b in the i-th iteration is a^i, b^i_{V*}, then we have:

$$\begin{aligned}
\Pr(b_S = 1) &= \sum_{i=1}^{\infty} \Pr(a^i = 1, a^1 = ... = a^{i-1} = 0, b^i_{V^*} = 1) \\
&= \sum_{i=1}^{\infty} (\frac{1}{2})^i \Pr(b^i_{V^*} = 1) \\
&= \Big(\sum_{i=1}^{\infty} (\frac{1}{2})^i\Big) \Pr(b_{V^*} = 1) = \Pr(b_{V^*} = 1)
\end{aligned}$$

Thus, the distribution of b is the same, and therefore the two distributions are indistinguishable.