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. Since all k messages sent from Merlin to Arthur are parallelized, we can consider the k messages as a single message m. Then the parallelized protocol is equivalent to the original AM protocol, where Arthur sends a random string and Merlin replies with k witnesses.

Let E_i be the event that Arthur accepts $x \notin A$ in the i-th copy. Formally, $E_i = (\exists P_0^*) \Pr(\langle P^*, V\rangle(x) = 1) > 1/2$. Then the probability that Arthur accepts x in the parallelized protocol is

$$\begin{aligned}\Pr(\text{Arthur accepts } x) &= \Pr(\bigcap_{i=1}^{k} E_i) \\ &= \Pr(E_1) \cdot \Pr(E_2 \mid E_1) \cdots \Pr(E_k \mid \bigcap_{i=1}^{k-1} E_i).\end{aligned}$$

Though the Merlin messages are not independent, we can still bound the probability for the j-th term $\Pr(E_j \mid \cap_{i=1}^{j-1} E_i)$. Due to the fact that Merlin would not receive any reply after Arthur first sent the random string, the j-th term is at most $1/2$. Therefore, the probability that Arthur accepts $x \notin A$ in the parallelized protocol is at most $1/2^k$.

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 $G = \pi(G_a)$.

Randomly sample $b \in \{0, 1\}$.

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 because it does not simulate the verifier's random tape. The verifier's random tape is used to generate the challenge b in the protocol. This simulator doesn't even use the verifier to determine its output!

It is a plain guess-and-check simulator that outputs the transcript if the guess is correct, independent of that G is isomorphic with G_b. The transcript does not have the same distribution as the real interaction between the verifier and the prover. This is not zero-knowledge because the simulator does not simulate the verifier's behavior at all.

(b) Consider a simulator S that works as follows:

Choose $a \in \{0, 1\}$ uniformly at random.

Sample a random permutation π and compute $G = \pi(G_a)$.

Randomly sample r and simulate V^* with r as the random tape.

If V^* sends $b = a$, output (G, π) as the message and the random tape r as the internal randomness.

If V^* sends $b \neq a$, rewind and start from the beginning.

We need to show that the output of the simulator S is indistinguishable from the real interaction between the verifier V^* and the prover P. It is clear that the output of S is identically distributed to the real interaction because a is chosen uniformly at random and π is a random permutation. The only difference is that S simulates the verifier's behavior with a random tape r, which will make no difference as V^*'s tape is also chosen uniformly at random.

In addition, S runs in expected polynomial time since the probability that it needs to rewind is $1/2$. This is because the probability that $b \neq a$ is $1/2$ due to the fact that a is chosen uniformly at random, independent of V^*.