Summary of Lecture 20

**Reading:** Katz’s Lecture Note 17.

- We derive an AM protocol for the graph non-isomorphism (GNI) problem and use that to show if the graph isomorphism (GI) problem is NP-complete, then the polynomial hierarchy collapses to the second level.

- The first observation is that the size of the following set would be different between the cases when $G_0$ and $G_1$ are isomorphic or not.

$$W = \{(H, \sigma) : H \text{ is isomorphic to either } G_0 \text{ or } G_1, \text{ and } \sigma \text{ is an automorphism of } H\}.$$  

For graphs with $n$ vertices, $|W| = 2n!$ when $G_0$ and $G_1$ are not isomorphic to each other; $|W| = n!$ when they are.

- We use the Goldwasser-Sisper set lower bound protocol (a general form in [Arora-Barak]; Katz’s lecture note contains a simple instance) to distinguish between the two cases, with the help of pairwise independent hash functions.