CMSC 652, Complexity Theory
Fall 2017, University of Maryland

Lecture on October 26th, 2017
Date: October 27, 2017

Summary of Lecture 18

Reading: Katz's Lecture Note 16.

- We start to cover interactive proofs, an important topic in computational complexity.
- Interactive proofs extend from NP by adding *randomness* and *interaction*. We introduced an example of a simple counting problem (e.g.., how many leaves are there in a picture?) with a three-message interaction protocol to solve.
- We formulate the complexity class IP, and its completeness, soundness, and allowed resources (BPP for the verifier, with polynomial-size messages, at most polynomial-round interactions).
- If there is no randomness, then IP reduces back to NP, simply because the prover can then generate the whole interaction and send it to the verifier to check.
- We don't know yet whether IP can really be more powerful than NP, as IP=PSPACE vs NP is an open question.
- However, we can use IP as a tool to study interesting problems, such as the graph iso-morphism (GSI) or the graph non-iso-morphism (GNI) problem.
- In particular, there is a two-message IP protocol that solves the GNI problem.