**IP = PSPACE**

Graph Isomorphism has a 2-round Interactive Proof.  

\[ \text{Graph Isomorphism} \in \text{CoNP} \text{ (not known to be in NP):} \]

- Input \( G_1, G_2 \)
- \(? \) is \( G_1 \neq G_2 \)

Although we know of no short way to "prove" that two graphs are not isomorphic, it is possible to interact with a powerful oracle, so that the oracle can convince you with overwhelming confidence that two graphs are not isomorphic. In this example, let's call the oracle "Endre".

Repeat 90 times
- Flip a coin \( c \in 1, 2 \)
  - Compute a random permutation of \( G_c \) and call it \( G \)
  - ask Endre: Is \( G \equiv G_1 \) or \( G \equiv G_2 \)
  - If \( G_1 \) and \( G_2 \) are not isomorphic, Endre will answer \( G \equiv G_c \) (with correct value of \( c \))
  - If they are isomorphic Endre will answer \( G \equiv G_c \) ? with 1/2 chance for \( c \)

An Interactive Proof consists of a verifer \( V \).

\( V \) is a proof system for a language \( A \) if:

\[ X \in A \Rightarrow \exists \text{prover}(P) \text{ Prob}(V(\text{accepts } X \text{ when interacting with } P)) = 1 \]

\[ X \notin A \Rightarrow \forall \text{prover}(P) \text{ Prob}(V(\text{accepts } X \text{ when interacting with } P)) \leq 1/4 \]

The protocol can be modified so that the prover sees the random coin flips. Interactive protocols where all coin flips are public are called "Arthur-Merlin' games. Arthur-Merlin games are used to define the class AM.

Thus, Graph Isomorphism \( \in \text{CoAM} \subseteq \text{CoNP}/\text{Poly} \)

Thus, Graph Isomorphism is not NP-complete, unless PH collapses.

For the proof of \( IP = PSPACE \), (this is NOT the actual interactive protocol which will be presented in a later lecture, but instead is a first
attempt at an interactive protocol, to show some of the main ideas.) Here is a complete problem for $PSPACE$:

Input: Arithmetic sequence $\psi$ of the form:

$$\Sigma_{X_1 \in 0,1} \Pi_{X_2 \in 0,1} \ldots \Sigma_{X_n \in 0,1} \psi(X_1 \ldots X_n)$$

Question: Is $\psi \neq 0$?

We will give an interactive proof for this problem:

Prover sends a prime $P$, a proof that $P$ is prime and a number $C$ and we claim $\psi \equiv C \pmod{P}$

If $\psi = \Sigma_{X_1 \in 0,1} \psi'$

Note that $\psi = \psi'(1) + \psi'(0)$

We will guarantee (inductively) that $\psi'(X_1)$ is polynomial of degree $n^{O(1)}$ in $X_1$.

The prover will send coefficients $d_0, d_1, \ldots, d_r$, s.t. $\psi'(X_1) = \Sigma_{i=0}^{r} d_i X_1^i$.

The verifier checks that $Q(0) + Q(1) \equiv C \pmod{P}$, if so, then verifier picks a random $Z$ and asks prover to prove that $\psi'(Z) \equiv Q(Z) \pmod{P}$

Reference: [Shen], J. ACM. vol 39, Oct 92, 878-880