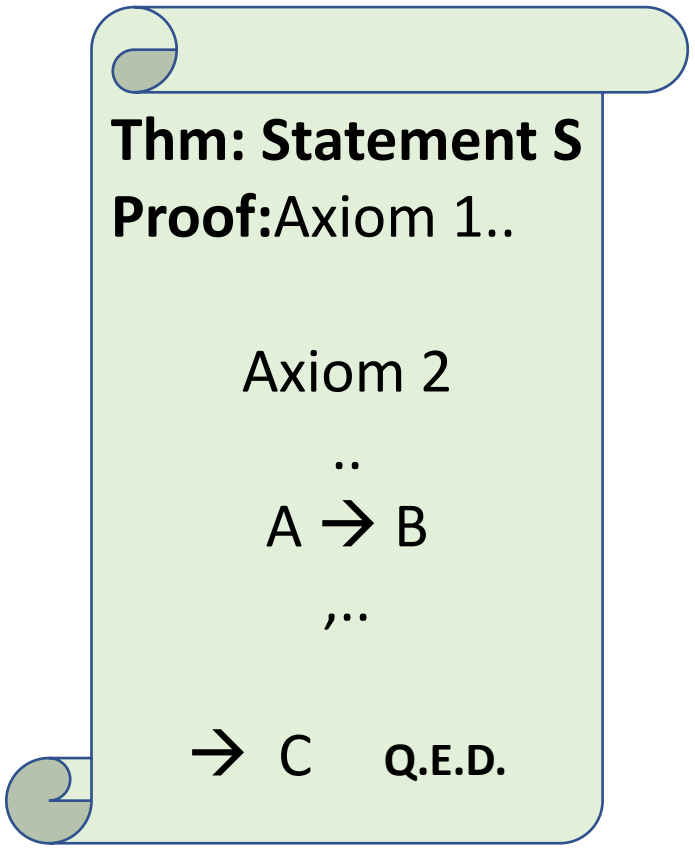
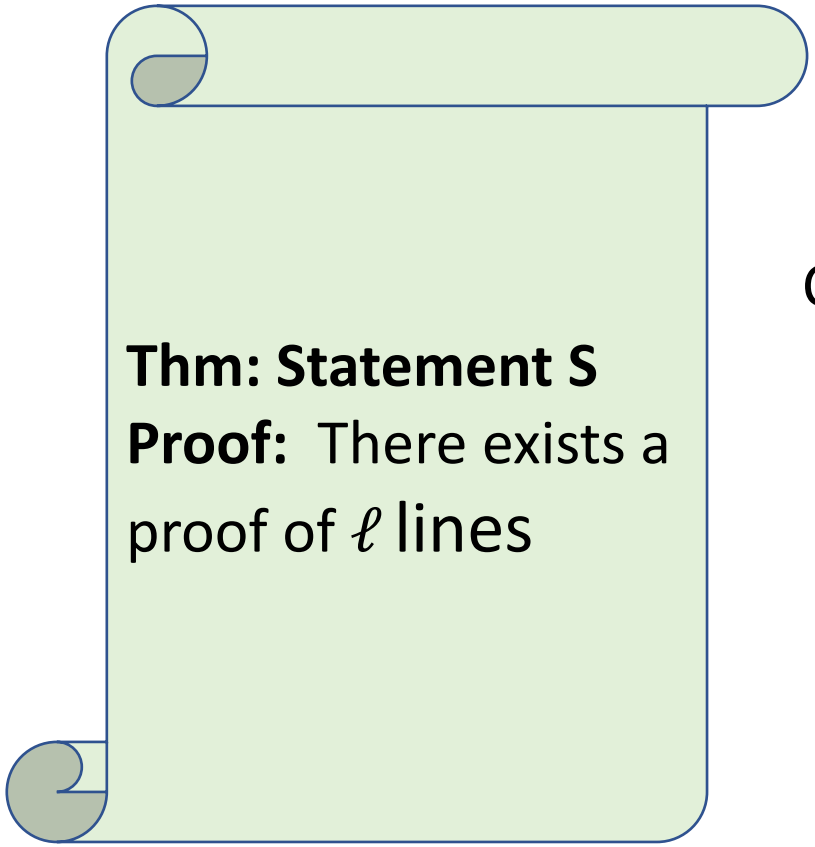
# Proofs

# What's a proof?

Checkable in $Poly(\ell)$ time,




$\ell$ lines long



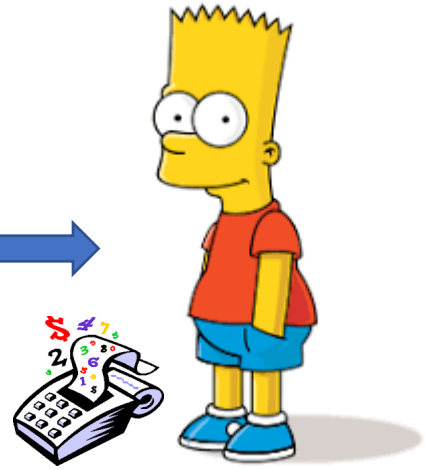

Checkable in $2^{\ell}$ time.

Statement Φ
(to be proved)

**PROVER**

**PROOF**

**Verifier**



ACCEPT /REJECT

***True Statements Are Provable***

- Φ is true

➔

∃ strategy such that Prover will Win/ Verifier will Accept.

***False Statements Cannot Be Proved***

- Φ is false

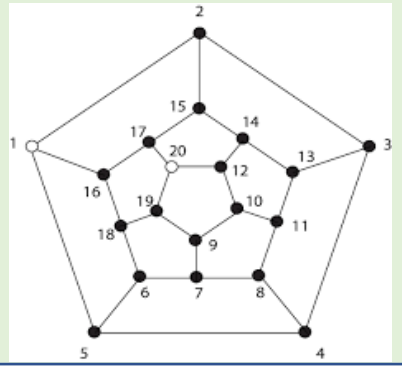
➔

∀ strategy of Prover, Verifier will Reject.

# NP

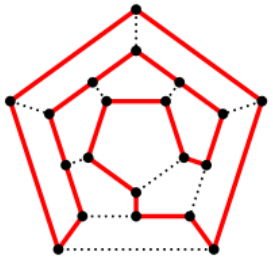
**Statement:**

*This graph has a Rudrata cycle”*




**PROVER**

**PROOF:**

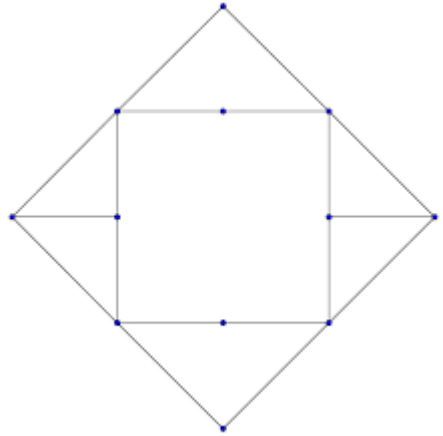


**Verifier**

**Polynomial-time computation**

ACCEPT /REJECT

# coNP = complement of NP

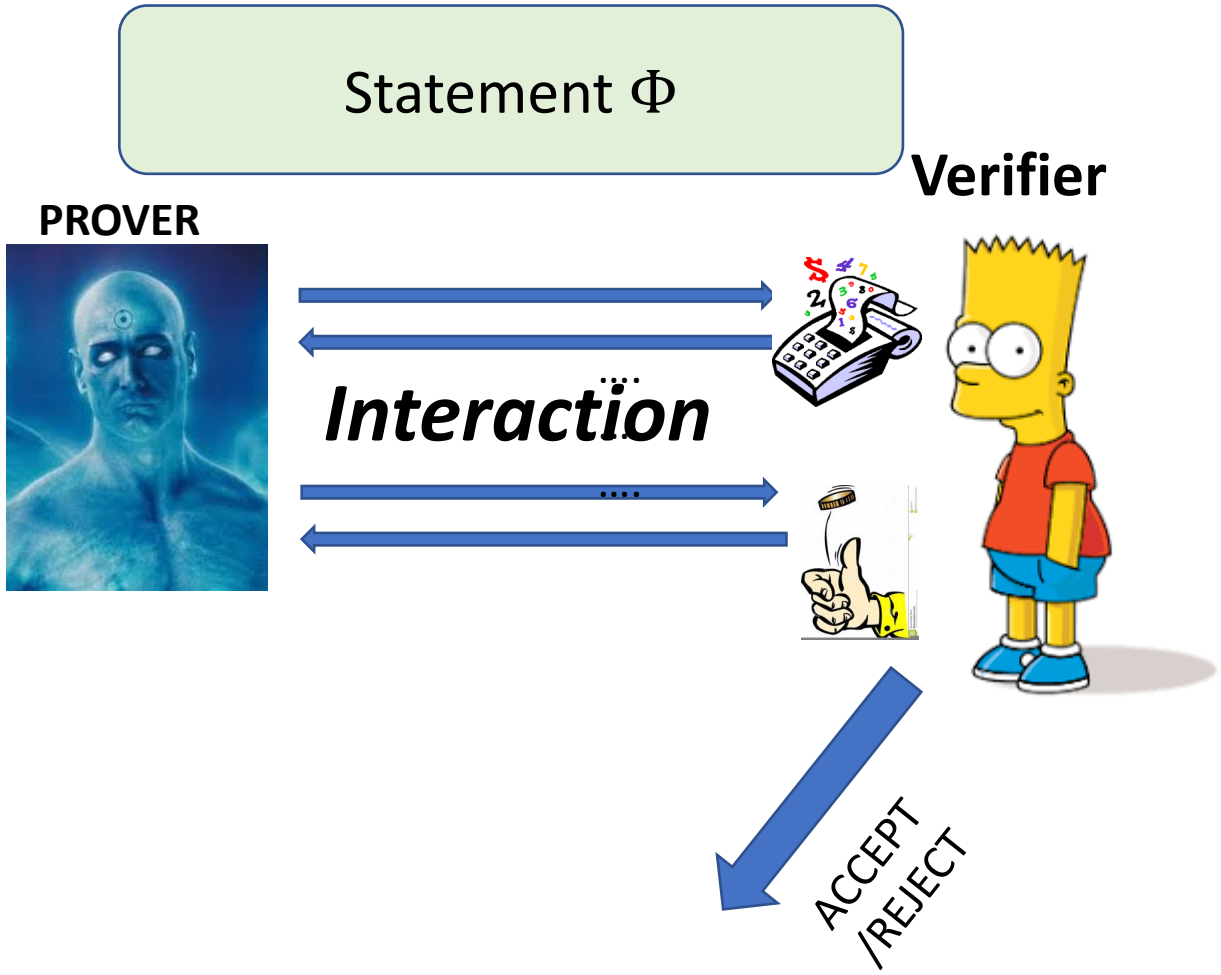


**Example:** *"This graph has NO Rudrata cycle"*

No efficiently verifiable proofs of truth of coNP statements in general.

However, if statement is false, there is an efficiently verifiable proof of "NOT $\Phi$".

# Interactive Proofs




***True Statements Are Provable***

- Φ is true

➔

∃ strategy such that Prover will Win/ Verifier will Accept.

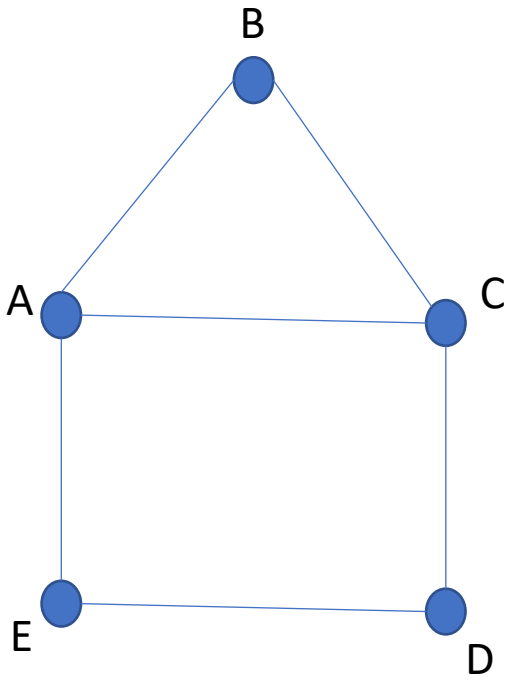
***False Statements Cannot Be Proved (with high probability)***

- Φ is false

➔

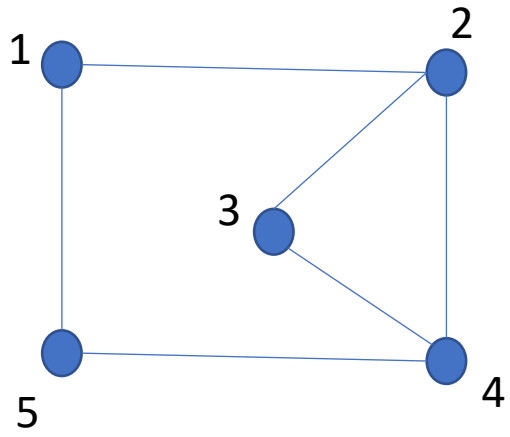
∀ strategy of Prover, Verifier will Reject with high probability (say 0.999) .

# Are these two graphs different?




| | |
|---|---|
| A | 2 |
| B | 3 |
| C | 4 |
| D | 5 |
| E | 1 |

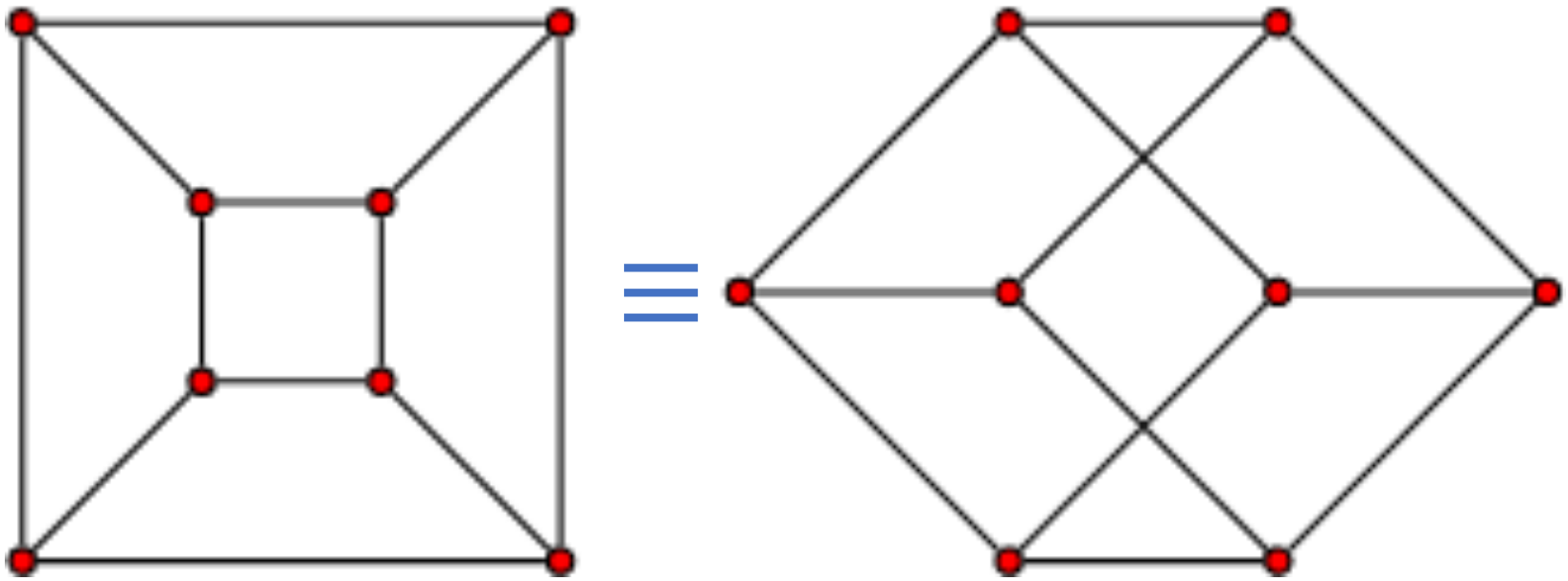
≡




*"Two graphs are isomorphic"*

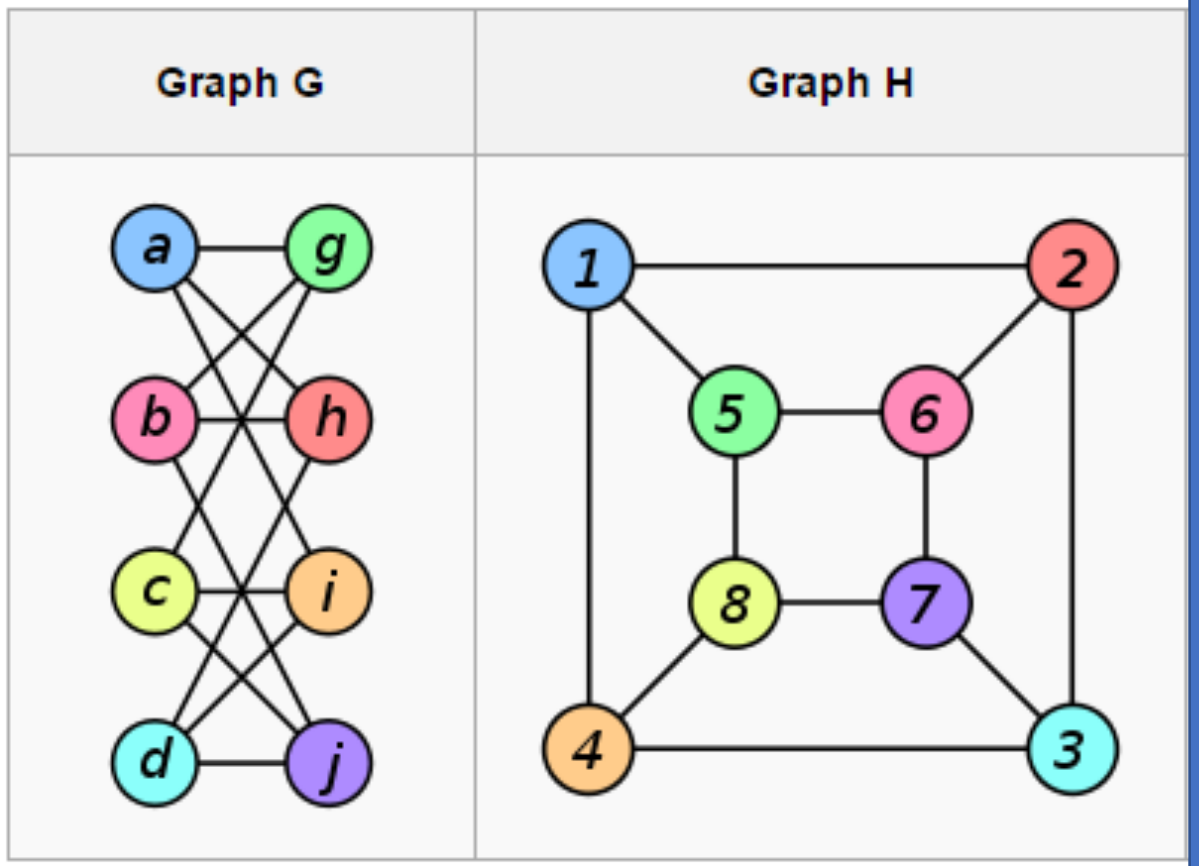
**Definition:** Graphs **G** and **H** are isomorphic if there exists a bijection $\pi$: $V(G) \to V(H)$ such that, $(i,j) \in E(G)$ if and only if $\big(\pi(i), \pi(j)\big) \in E(H)$

# Are these graphs same?



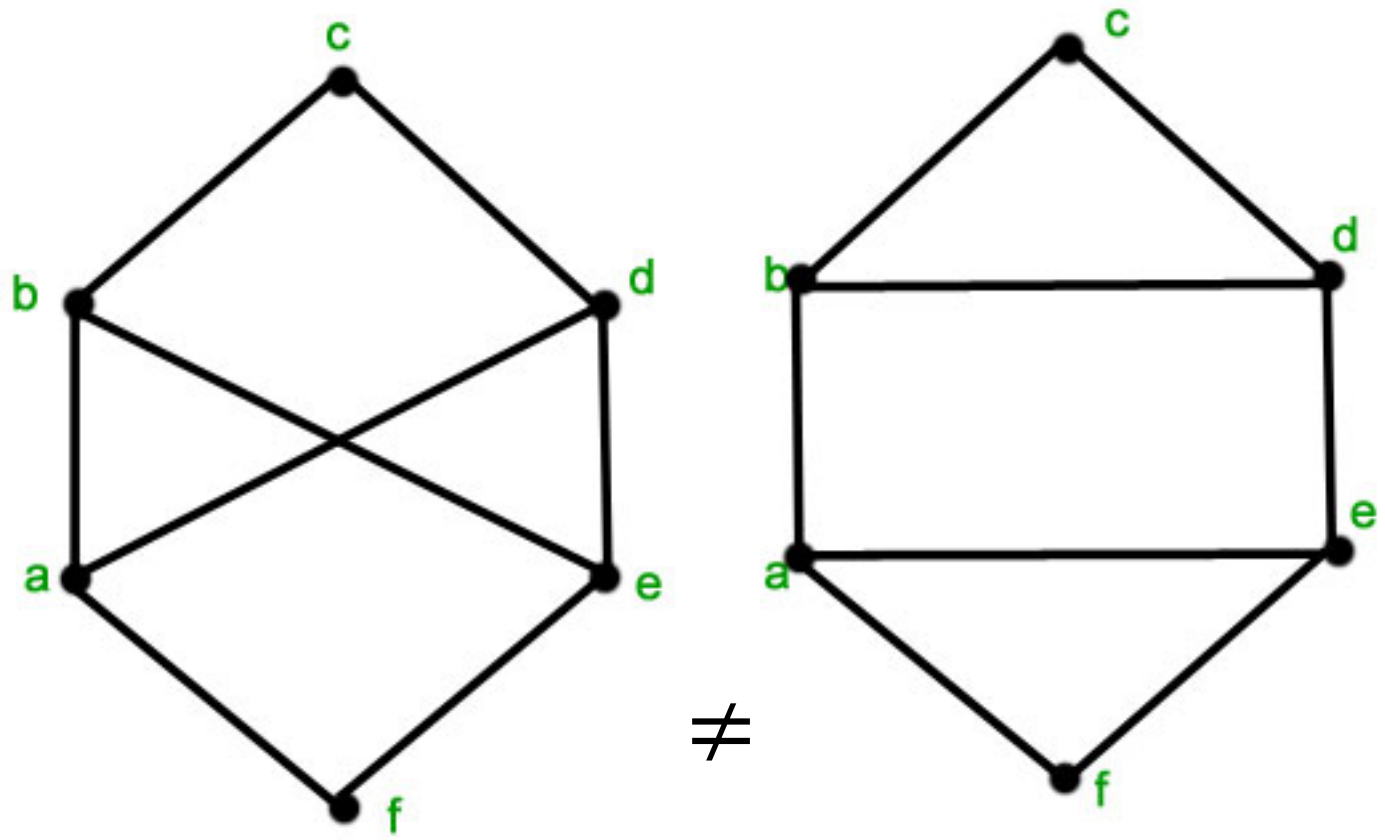
**G** **H**

# Graph Isomorphism




**Theorem:** Graph Isomorphism is in NP

# Are these two graphs isomorphic?




Can you prove it?

Graph Isomorphism is in NP:

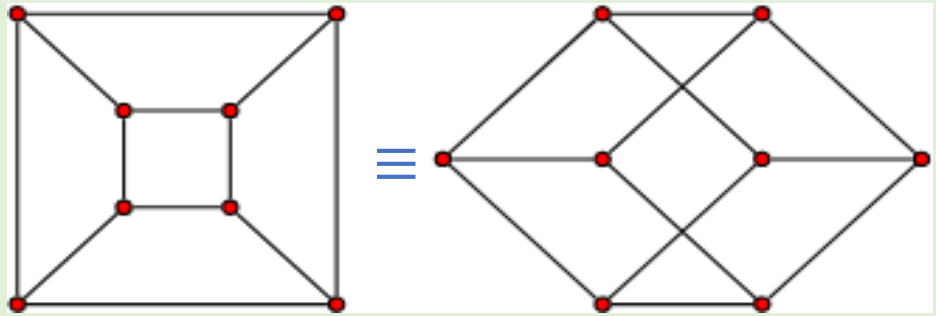
Its easy to prove that $G \equiv H$

Graph Non-Isomorphism is in coNP

Its not easy to prove to a verifier that $G \not\equiv H$

# Graph Isomorphism: NP Proof

**To Prove:**



**G** **H**

**PROVER**

**Verifier**

**PROOF:** Bijection $\pi: V(G) \rightarrow V(H)$

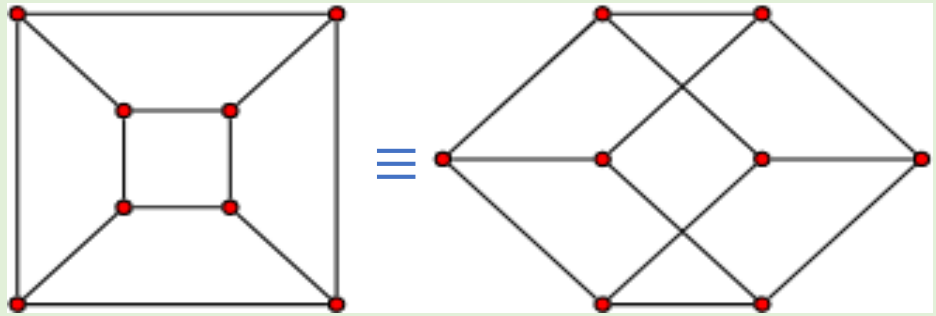
**Polynomial-time computation**

ACCEPT /REJECT

Prover is revealing too much information??

# Graph Isomorphism: NP Proof

**To Prove:**



**G** **H**

**PROVER**

**Verifier**

# Proving Graph Non-Isomorphism

**To Prove:** Graph G $\not\equiv$ *Graph H*

**PROVER**

**Verifier**

# Proving $Coke \not\equiv Pepsi$

**PROVER**

Pick Coke or Pepsi at random

**Verifier**

It is Coke/Pepsi!

**True things can be proved**
If $Coke \neq Pepsi$ , then prover can succeed each round.

**False things can't be proved**
If $Coke \equiv Pepsi$ , then prover fails each round with probability $\frac{1}{2}$.
Repeat $k$ times, probability of failure $1 - 1/2^k$

# Proving Graph Non-Isomorphism

**To Prove:** Graph G $\not\equiv$ *Graph H*

**PROVER**

**Verifier**

1. Randomly pick $G$ or $H$, say $\Gamma =$ $G$ or H with probability $\frac{1}{2}$
2. Randomly permute the vertices of graph $\Gamma$ to get $\pi(\Gamma)$

send $\pi(\Gamma)$

Graph G or H

1. Accept if prover correctly guesses whether $G$ or $H$ is used

**False things cannot be proved:**

If $G \equiv H$, then $\pi(\Gamma)$ has the same distribution, whether verifier chose $G$ or $H$

# What more can be proved interactively??

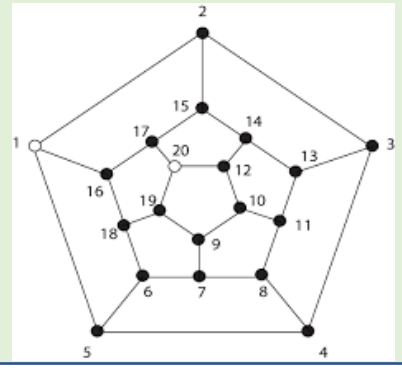
## IP = PSPACE!!

- Formula $\Phi$ is not satisiable
- Formula $\Phi$ has exactly $k$ satisfying assignments
- There is a winning strategy for Black in Chess

# Sampleable Proofs

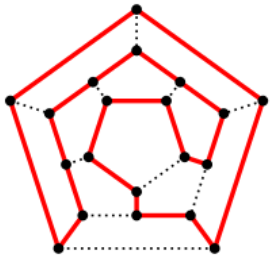
**Statement:**

*This graph has a Rudrata cycle”*




**PROVER**

**Special PROOF:**



**Verifier**

**Samples only three bits o proof**

ACCEPT /REJECT

**PCP Theorem:** Every NP statement has a sampleable proof

# More and more proofs..

- Multi-prover interactive proofs
- Quantum prover/Classical verifier
- Quantum multiprover/classical verifier..
- … weak verifier

..