NP: Class of decision problems w/ poly-time verifiable proofs
   "witnesses"
   \[ L = \{ x \in \{0,1\}^* \mid \exists \pi : V(x, \pi) = 1 \} \]

\[ P \xrightarrow{\text{proof}} \text{Verifier} \]

Define "proof system" for lang. L:
- Completeness: "true assertions have proofs"
  \[ x \in L \Rightarrow \exists \pi : V(x, \pi) = 1 \text{ and } \pi \in \text{poly}(|x|) \]
- Soundness: "false assertions have no proofs"
  \[ x \not\in L \Rightarrow \forall \pi : V(x, \pi) = 0 \]

3-Coloring:

3-COL: \{ G : G is 3-colorable \}
3-COL \in NP:

\[ P \xrightarrow{\text{proof}} \text{Verifier} \]

Interactive Probabilistic Proofs
- Completeness:
  \[ x \in L \Rightarrow \Pr[\text{Verifier}(x) = 1] \geq 1 - \epsilon(n) \]
- Soundness:
  \[ x \not\in L \Rightarrow \forall \pi : \Pr[\text{Verifier}(x, \pi) = 1] \leq \epsilon(n) \]

NP \subseteq IP
IP = PSPACE

IP for 3COL:

\[ P(G, \pi) \]

w.h.p. reveal all of \( c(v_i) \)

- Completeness: \( \omega \text{ 3-colorings } \Rightarrow c(v_i) \neq c(v_j) \)
  \[ \text{edges } (v_i, v_j) \]
- Soundness: \( \omega \text{ not 3-coloring } \Rightarrow \exists \text{ edge } (v_i, v_j) \)

\[ \Pr(\text{Verifier}) \geq \frac{1}{m^{100}} \]

\[ \Pr(\text{never fail click}) \geq \left(1 - \frac{1}{m^{100}}\right)^{100 m} \]
**Zero Knowledge Interactive Proof**

\[ P \xrightarrow{P_1} V \]
\[ x, w \xrightarrow{V_1} x, w \xrightarrow{V_2} \]

**Definition (P, V) (honest-verifier) zero-knowledge if**

\[ \exists S \ni \forall x \in L \quad \text{View}_V(P(x, w) \equiv V(x)) \approx S(x) \]

transcript V sees but P proof computationally indistinguishable

(P, V) zero-knowledge

\[ \forall V' \exists S' \forall x \in L \quad \text{View}_V(P(x, w) \equiv V'(x)) \approx S'(x) \]

V might try | hold \[\rightarrow\] simulate S depends on V

**ZKP for 3COL:**

\[ P(x) \]
\[ \prod \text{random arithmetic chords} \]

\[ e = (v_i, v_j) \]

\[ \text{open}(\prod c(v_i), \text{open}(\prod c(v_j))) \]

\[ \text{check}\ \prod c(v_i) \not\equiv \prod c(v_j) \]

\[ \text{Repeat 100m times} \]

- Completeness: same as before
- Soundness: same as before
- Zero knowledge:
  simulate: Guess edge \( e = (v_i, v_j) \) that will be queried by V
  - Correct, check guesses \[\Rightarrow\] include in transcript
  - Incorrect, re-void | don't include transcript

\[ P(S \text{ guesses correct edge } = \frac{1}{m}) \approx 100 \text{ m}^2 \text{ rounds until simulated proof} \]
Graph Isomorphism

\[ L \subseteq \Sigma^* \text{ s.t. } G \equiv H \iff \exists \pi \in \Pi(G) \]

\[ \begin{array}{c}
\Phi(G, H, c) \xrightarrow{c \in [0, 1]} V(G, H) \\
\left\{ \begin{array}{ll}
\text{if } c = 0: & 5 \\
\text{if } c = 1: & 5 \cdot \pi^{-1}
\end{array} \right.
\end{array} \]

Complexity:
- \( G, H \) isomorphic: check always succeeds

Soundness:
- \( G, H \) not isomorphic:
  - check only succeeds if \( c = 0 \)
  - \( \Pr(\text{success}) = \frac{1}{2} \)

Zero-knowledge:
- Simulator:
  \[ \begin{array}{c}
\Sigma(G, H) \xrightarrow{c \in [0, 1]} V(G, H) \\
\left\{ \begin{array}{ll}
\text{if } c = 0: & 5 \cdot G \text{ if } c = 0 \\
\text{if } c = 1: & 5 \cdot H \text{ if } c = 1
\end{array} \right.
\end{array} \]

\[ \Pr(\text{success}) = \frac{1}{2} \Rightarrow 2 \cdot 100 \text{ steps to transcript} \]

Thus Every NP-language has ZKIP

\[ \begin{array}{c}
\text{Pf: 3-coloring is NP-complete.} \\
\text{Given } x \text{ construct } G \text{ s.t. } G \text{ 3-colorable } \iff x \in L
\end{array} \]
Zero-knowledge proof of knowledge for Discrete Log (schnor)

"Proof of knowledge": P "knows" a witness 
(regards soundness)

Let "knowledge soundness with error ε"

\[ \forall \text{ prov-}P' \; \forall x \]

If \( P' \) is honest \( P' \) halts \( P'_{\text{VK}}(P', V(x, r)) = \text{accept} \) \( \Rightarrow c+\epsilon \]

3 algorithm \( \mathcal{E} \) (knowledge extractor) running in time poly \( \frac{1}{\epsilon} \):

\[ \mathcal{E}(x) = w \; \text{wp.} \frac{1}{2} \]

Schnorr proof of knowledge for discrete log

Choose \( q \) a generator

\[ h = g^x \]

\[ g^b \]

\[ a = g^r \]

\[ V \]

\[ (g, h) \]

\[ b \]

\[ b \in \mathbb{Z}_q \]

\[ c = r + xb \]

\[ ah^b = g^c \]

Complexity: \( \mathcal{V} \)

Proof of knowledge: \( P \) runs protocol twice and sees \( a \) (rounding)

\[ (a, b, c), (a', b', c') \]

\[ b \neq b' \]

\[ c = c' \]

\[ ah^b = g^c \]

\[ ah'^b = g^{c'} \]

\[ h^{-b} = g^{c'} \]

\[ x = c \cdot c' \div b \cdot b' \text{ mod } q \]

Honest-verifier zero-knowledge:

\[ \text{simul}: (b, c) \in \mathbb{Z}_q \]

\[ \text{set} a = h^{-b} \cdot g^c \]

Application: Identification scheme:

Observer learns nothing about secret \( x \)