th: (Goldwasser–Sipser) $IP[k] \subseteq AM[k+2]$.

lemma: Let $S \subseteq \{0,1\}^n$ be a set st prover can certify that $x \in S$. Let $k \in \mathbb{N}$. There is an AM proto st
$|S| \geq k \Rightarrow V$ accepts w/pr. $\geq 2/3$
$|S| \leq k/2 \Rightarrow V$ rejects w/pr. $\geq 2/3$.

$\mathcal{H} = \{h_0\}$, $h_i : \{0,1\}^n \to \{0,1\}^k$.

def $\mathcal{H}$ pairwise indep. hash if $\forall x \neq x' \in dom$; $\forall y, y' \in im$;
$\Pr_{h_i \in \mathcal{H}}[h_i(x)=y \wedge h_i(x')=y'] = 2^{-2k}$.

claim: $\mathcal{H}$ exists. //

obs implies uniform hashing:
$\Pr_{h_i \in \mathcal{H}}[h_i(x)=y] = \sum_{y'} \Pr[\wedge] = 2^k \cdot 2^{-2k} = 2^{-k}$.

protocol: let $k = \lfloor \log(2k) \rfloor$ (i.e. $2^{k-1} < 2k \leq 2^k$).

V	samples h and y.
P	sends x st $h(x)=y$ and cert. that $x \in S$. (or ~~x~~ if $\nexists$).
V	checks $h(x)=y$ and $x \in S$.

need to show: $|S| \geq k \to \Pr[\exists x \ldots] \geq p_1$
$|S| \leq k/2 \to \Pr[\exists x \ldots] \leq p_0$ $\quad p_1 - p_0$ dist.

well pick $p_0 = \frac{1}{2}\frac{k}{2^k}$, $p_1 = \frac{3}{4}\frac{k}{2^k}$. obs we don't get $2/3$ vs $1/3$; to make proto formally correct we'll do error reduction (in parallel).

(ii) is clear: $P_r = \frac{E|h(S)|}{2^k} \leq \frac{|S|}{2^k} \leq \frac{1}{2}\frac{k}{2^k}$

(i) follows from hashing properties. fix y.

$\Pr[\exists x\ h(x)=y] = \Pr[\bigcup_{x \in S_x} h(x)=y] =$ ← inclusion-exclusion

$= \sum_x \Pr[h(x)=y] - \sum_{x,x'} \Pr[h(x)=y \wedge h(x')=y]$

$= |S| \cdot 2^{-k} - \binom{|S|}{2} \cdot 2^{-2k} \geq$ ← $\leq \frac{1}{4}$

$\geq |S|/2^k - |S|^2/2^{2k+1} = |S|/2^k \left(1 - \frac{|S|}{2^{k+1}}\right) \geq \frac{3}{4} \cdot \frac{k}{2^k}$.

//

how to use for graph-non iso?

count # graphs isomorphic to G_1 and G_2. if non-iso, this will be double than if iso.

formally: $S = \{(H,\pi) : \pi \in Aut(H),\ H \cong G_1 \text{ or } H \cong G_2\}$.

obs: → $G_1 \cong G_2 \to S \cong S_n$.
→ $G_1 \not\cong G_2 \to S \cong \{1,2\} \times S_n$.
→ can certify $(H,\pi) \in S$ by giving permutation.

e.g. • — • (1)(2)(3)
• — • (1)(23)
• • — • (1)(2)(3)
• — • (12)(3)
• • (1)(2)(3)
• • (13)(2).

hence proto is:
distinguish between $|S| = 2n!$ or $|S| = n!$.

how to use for $IP[k] \subseteq AM[k+2]$?

problem: cannot easily verify $r \in S_x$: if P knows r, they can cheat.

let us see how to fix for $IP[2]$.

let $z_1 = V(x,r)$. P must certify that their message z_2 would be accepted by V for most of the rs that produce z_1, not only r.

assume for simplicity z_1 uniformly distributed among all messages of length ℓ. then proto is:
V samples $r \in \{0,1\}^m$ and sends r.
P sends z_1, z_2.
(P,V) check that $|\{r : V(x,r)=z_1,\ V(x,z_1,z_2,r)\}| \geq 2^{m-\ell} \cdot \frac{2}{3}$ (and not $\leq 2^{m-\ell} \cdot \frac{1}{3}$).

this is OK for simple protocols such as Graph-non-iso, but in general we could have
→ messages of different lengths.
→ messages not equidistributed.
we'll leave as exercises.