Nem-interaktív ZK bizonyítás
HH – körre:

[Következmény: minden NP-beli nyelvre van ilyen.

[Lemma: Van f egyirányú permutáció
$\{0,1\}^n \to \{0,1\}^n$-re

A bizonyítás két részben megy:
I. rész: fizikai modell, f-et így vesszük
II. rész: f-et használjuk, nem fizikai modell.

I. rész: Kapnak a játékosok ℓ db kétszer választott bitet, ezt azonban az ellenfél nem látja V, P látja az egészet.
$\ell = n^6$, egy A $n^3 \times n^3$-as 0-1 mátrix elemeinek felel meg:
$\Pr(a_{ij} = 1) = \frac{1}{n^5}$

Def: Azt mondjuk, hogy A hasznos, ha van egy $n \times n$-es, egyetlen ciklusból álló vész-permutációmátrixra, és az összes többi eleme 0.

Áll: A legalább
$$\Omega(n^{-\frac{3}{2}})$$
vsz-el hasznos.

biz: Az 1-esek számának várható értéke $n^6 \cdot n^{-5} = n$. $\Theta(n^{-1/2})$ vsz-el A pontosan n 1-est tartalmaz. A teljesen legyes sorában legfeljebb $\binom{n^3}{2}(n^{-5})^2 < n^{-4}$ vsz-el van egynél több egyes. Így legalább $1 - 2n^3 \cdot n^{-4} = 1 - \Theta(n^{-1})$ vsz-el minden sor és oszlop csak egy 1-est tartalmaz.

Így $O(n^{-1/2})$ vsz-el van benne $n!$-es permutációmátrix.

Nyilván $(n-1)!$ egyciklusú permutáció van. Így $\frac{1}{n} O(n^{-1/2}) = O(n^{-3/2})$ vsz-el lesz hasznos A.

(még mindig az 1. fázis)

A protokoll: Az $\ell = n^6$ db véletlen bitet V nem látja, ki vannak rakva az asztalra, de lefordítva, mintha kártyák lennének

input: G gráf

P megnézi G-t, ~~tegy~~ ebben ~~...~~ megtalál egy H-kört, ez a C.

A vagy hasznos, vagy nem.

Ha A hasznos:

– P felfedi V-nek a permutációmátrixon kívüli $n^6 - n^2$ bitjét

– P megkeresi a π_1 és π_2 leképezéseket, amelyek a $V(G)$-t úgy képzik le az $n \times n$-es permutációmátrix soraira és oszlopaira, hogy a C az egyesekre képződjön (azaz a H-kör az egyciklusú permutációra.)

– P felfedi a mátrix $n^2 - |E(G)|$ 0 elemét, amely a G nem-éleinek felel meg

– P megmondja a (π_1, π_2) párt

Ha azonban A nem hosszú, akkor P
kilépdi mint az $\ell = n^6$ bitet.

Mit csinál V?

– Ha P nem lépte ki mint az $\ell = n^6$ véletlen bitet, akkor V ellenőrzi, hogy a G összes nem-élét a (π_1, π_2) ⊗-ba vitte-e.
Ha igen, elfogad.
– Ha P kilépdte mint az $\ell = n^6$ bitet, akkor V ellenőrzi, hogy A valóban hosszú-e.

Ez miért jó?

– Ha G Hamilton ⇒ V elfogad, akár hosszú A, akár nem.

– Ha G nem Hamilton, A legalább $\Omega(n^{-3/2})$ valószínűséggel hosszú.
Ekkor $\pi_1(V) \times \pi_2(V)$-ban ha van egy ciklusú permutáció, akkor ellenőrzés, G tényleg Hamilton, mert G minden nem-élére megnézi, hogy 0-ra képződjön.
– ~~Ha nem az egy ciklusú permutáció,~~

Ha $\Pi_1(V) \times \Pi_2(V)$-ben nincs egyciklusú permutáció (bár A hozzá-os) akkor G adjacencia mátrixának valamely sorát vagy oszlopát elárulta P V-nek; ez nem csupa-0, tehát V nem fogadja el.

Tehát ha G nem Hamilton, akkor V legalább $\Omega(n^{-7/2})$ vsz-el elutasít.

Házi feladat: így ez tökéletes ZK

Hogy lehet a fizikait számítási ZK-vá tenni?

Legyen $f:\{0,1\}^n \to \{0,1\}^n$ bijektív, egyirányú fv (egyirányú permutáció)

$b:\{0,1\}^n \to \{0,1\}$, úgy, hogy $\Pr(b(x)=1) = \frac{1}{n^5}$ [ezeket V is tudja számolni]

a közös véletlen egy n^7 hosszú 0-1 sorozat: $y_1, y_2, \dots, y_{n^6}$, ahol $y_i \in \{0,1\}^n$

az $n^3 \times n^3$-as mátrix bitjei legyenek $b(f^{-1}(y_i))$, $i = 1, 2, \dots, n^6$.

„fellhívás": P előállja $f^{-1}(y_i)$-t V-nek.