SZÜLETÉSNAP-PARADOXON / TEKNŐS-NYÚL

2025-12-08

SZÜLETÉSNAP-PARADOXON

k ember : $\text{Prob}\left(\exists x \neq y : x \text{ és } y \text{ szül.napja azonos}\right) = ?$

modell : 365 nap $\quad \frac{1}{365}$

Egzakt:

$$1 - \text{Prob}(\text{csupa különböző})$$

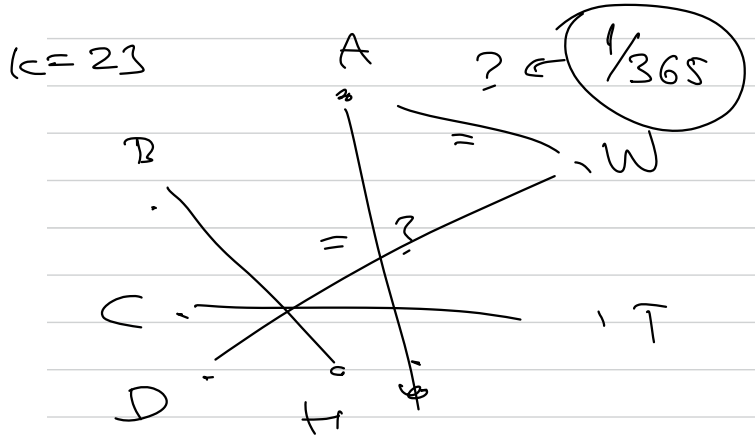
$$\frac{\binom{365}{k} \cdot k!}{365^k} = \frac{365 \cdot 364 \cdot \ldots \cdot (365-k+1)}{365^k}$$

Kérdés: $k = ?$ $\quad \min$ $\quad \text{Prob}(\ldots) > 50\% \longrightarrow \boxed{k = 23}$

$365 \to N$ $\quad$ 50% : $k \sim c \cdot \sqrt{N}$

↑
bizonyítható

$k = 23$



Minden párra van egy kisi esély, hogy $=$

$\frac{1}{365}$

$\binom{23}{2}$ eset közül ha bármelyik

teljesül $\Rightarrow$ baj

$\binom{23}{2} = 23 \cdot 11 = 253$

$\text{Prob}(A_1 \cup A_2 \cup \dots A_{50\%}) \neq \text{Prob}(A_1) + \dots + \text{Prob}(A_{50\%})$

$<$

Hash-függvények:

ALGO D.S.

CRYPTO

$H: \{\text{sok mindé}\} \longrightarrow \{\text{kevesebb dolog}\}$

pl. $\{0 \dots N\} \to \{0 \dots u\}$

$\{\text{STRING}\} \to \{0,1\}^{256}$

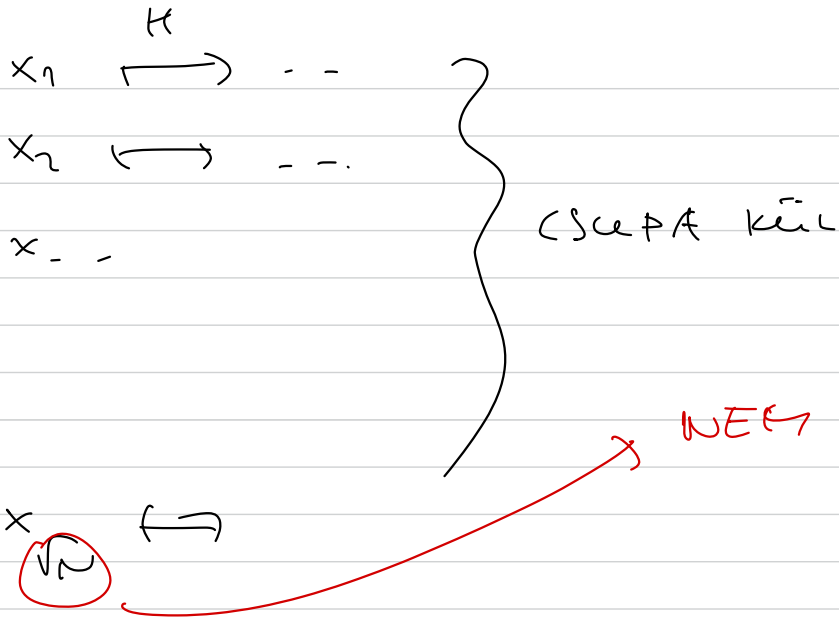
„CÉL": különböző x, x' : $H(x) \neq H(x')$

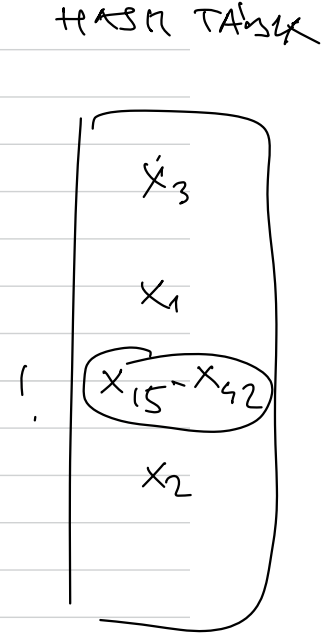
nagy valószínűséggel.

SZÜL. NAP.: $\text{img}(H) \sim N$

$\sim \sqrt{N}$ db értéknél <u>lesz</u> ütközés valószínűség

COLLISION





LD.: PERFECT HASH

Mikor lehet jó egy ütközés

1.) RUBIK

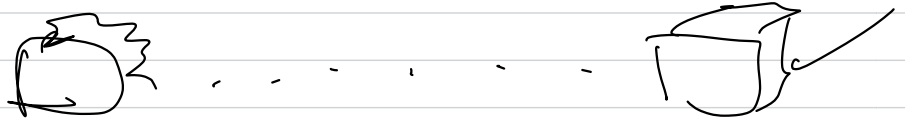
2) PRÍMFAKTORIZÁCIÓ

Leggyorsabb kirakás?

20 lépés a max

ALGO:

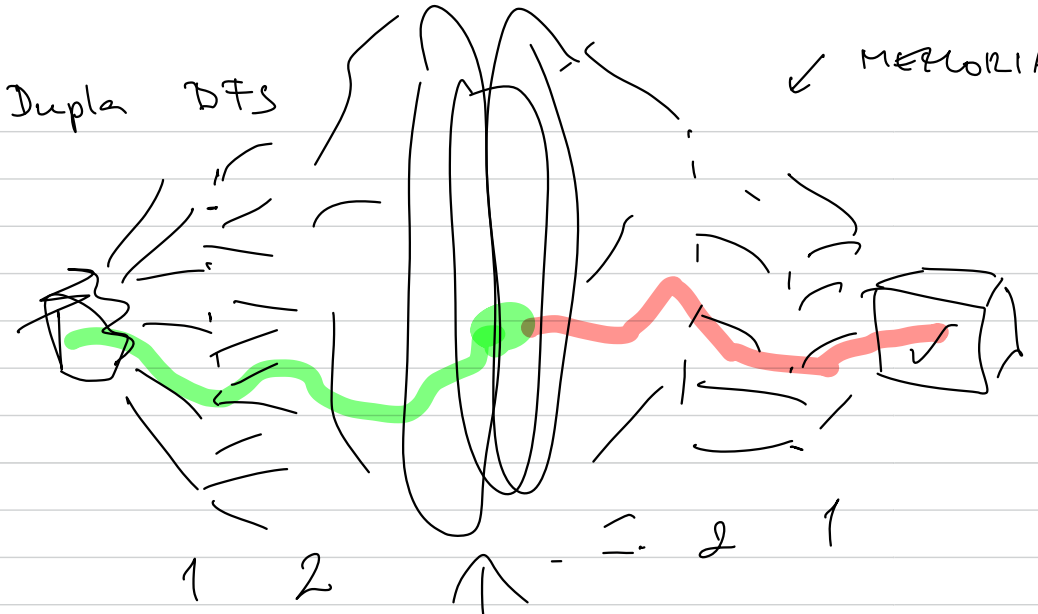
konkrét állás ⟷ kirakott állás



G graf,
s-t shortest path

túl nagy

BFS?? MEMÓRIA PROBLÉMA



ÜTKÖZÉS: LEVEL 8 vs LEVEL 8.

16

CÉL: ÜTKÖZÉS KERESÉSE A BFS-FÁBAN.

FAKTORIZÁCIÓ

POLLARD-FÉLE ρ algoritmus. CÉL: ÜTKÖZÉS KERESÉSE

ALAPÖTLET: $N = p \cdot q$ (p, q prímek, de nem tudjuk, mik)

Random x-ek modulo N

$$x_1 \xrightarrow{\bmod p} y_1$$
$$x_2 \longmapsto y_2$$
$$\vdots \qquad \vdots$$
$$x_k \longmapsto y_k$$

ELV (SZÜL. NAP):

$k \sim \sqrt{p}$: $\exists$ ütközés

$y_i \equiv y_j$ kongruens mod p

$LNKO(x_i - x_j, N)$: P jószínű

ALGO (1. változat)

$x_1, x_2, \dots, x_k$ random, $\forall i,j$: LNKO$(x_i - x_j, N)$

osztható p-vel: ✓

ÜTKÖZÉS (mod p): JÓ

CÉL: ütközésdetektálás

ABSZTRAKT FELHOZÁS:

x_0 adott

$x_0 \in X$ $\quad f: X \to X$ adott

$x_0 \overset{f}{\mapsto} x_1 \overset{f}{\mapsto} x_2 \overset{f}{\mapsto} \dots$

$x_0, x_1, \dots$ sorozat: x_0

$x_1 = f(x_0)$

$x_2 = f(x_1)$

$\vdots$

FELADAT: i, j: $x_i = x_j$

0. megoldás: $\forall i$-re: $x_i = x_{i-1}$? $x_i = x_{i-2}$? ... $x_i = x_0$?

$H = \{x_0\}$

$i := 0$

$x_{i+1} := f(x_i)$

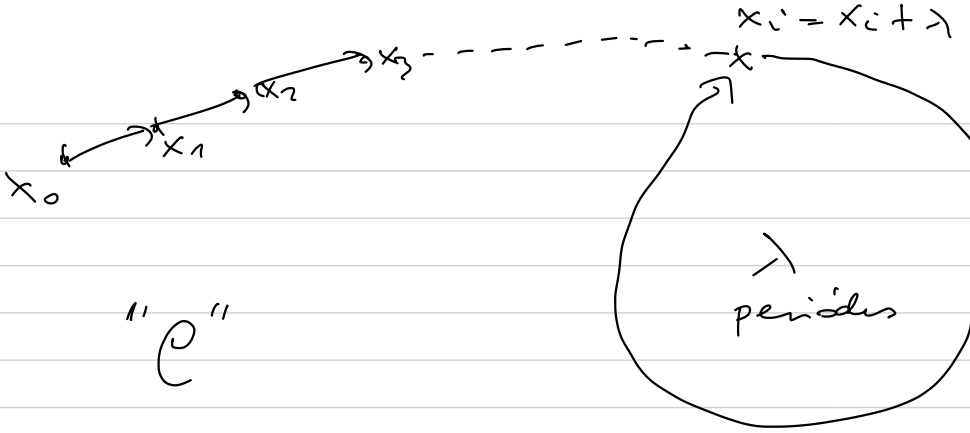
if $x_{i+1} \in H \longrightarrow$ HURRÁ

else $i := i+1$; $H := H \cup \{x_{i+1}\}$

MEMÓRIA!

KONSTANS TÁR: FLOYD-FÉLE PERIÓDUSKERESÉS (A.K.A TORTOISE AND HARE)

ÖTLET: $x_0, x_1, \ldots$ sorozat: (X véges)



"ρ"

$x_i = x_{i+\lambda}$

$x_{i+1} = x_{i+\lambda+1}$

$\vdots$

$x_j = x_{j+\lambda}$

ha $\boxed{j \geq i}$

ha $m \cdot \lambda > i \Rightarrow x_{(m\lambda)} = x_{(m+1)\lambda} = x_{(m+2)\lambda} = \dots = x_{(2m\lambda)}$

$x_{m\cdot\lambda} = x_{2m\lambda}$

$\exists$ index: j $\quad x_j = x_{2j}$

ALGO: $x_0, y_0 := 0$

CIKLUS:

$x = f(\text{előző } x)$, $y = f(f(\text{előző } y))$ // x_i, $y_i = x_{2i}$

ha $x == y$: NINCS CIKLUS

POLLARD ρ: $f: x^2+1 \mod N$

$x_0 = 2$ pl. $x = x_0$; $y = y_0$

CIKLUS:

$x = f(x)$

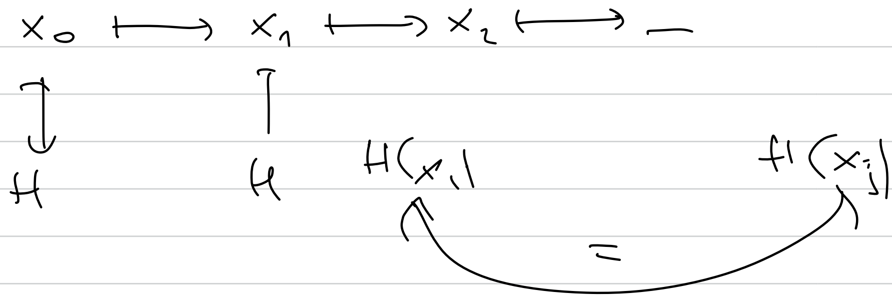
$y = ff(y)$

if $LNKO(x-y, N) \notin \{1, N\}$ → NTRÉS

RUBIK / HASH ütközés: f pszeudo random függvény

CÉL: $X \xrightarrow[f]{H} X$: x, x': $f(x) = f(x')$ $x \neq x'$

MEMÓRIAIGÉNY KICSI:



$$x_{i+1} = f(H(x_i))$$

$$x_{i+2} = f(H(x_{i+1}))$$ .. Jdl..

<u>cél</u> : $h(x_i) = h(x_j)$ ← FLOYD $(2 \cdot i = j)$