



# ÚJ ELVŰ SZÁMÍTÁSOK AZ INFORMATIKÁBAN

BEVEZETŐ A KURZUSHOZ, 2023

GAZDAG ZSOLT

SZTE, SZÁMÍTÁSTUDOMÁNY ALAPJAI TANSZÉK

# A KURZUSRÓL

- **Előadó:** Gazdag Zsolt
- **Elérhetőség:** Irinyi épület, III. lh. 67. szoba
- **Email:** [gazdag@inf.u-szeged.hu](mailto:gazdag@inf.u-szeged.hu)
- A kurzus **teljesítésének** feltételei:
  - A vizsgán egy írásbeli teszt (**beugró**) teljesítése:
    - Kis kérdések a feltöltött előadás-fóliasor alapján; rossz válaszáért pontlevonás
    - A **sikeres** beugró legalább 50%-os
  - Sikeres beugró esetén **szóbeli vizsga**

# A KURZUSRÓL

- **Félévközi munkával** megajánlott jegy kapható
  - Öt kisdolgozat az előadás helyén és idejében: okt. 4, 25, nov. 15, 29, dec. 13.
    - Ha a négy legjobb mindegyike legalább
      - 60% -> közepes
      - 70% -> jó
      - 85% -> jeles a megajánlott jegy
  - Egyébként a kisdolgozatok átlagának bizonyos része **hozzáadódik a beugróhoz**

# MOTIVÁCIÓ: A BONYOLULTSÁGELMÉLET EGYIK ALAPKÉRDÉSE

Problémák, melyek  
polinomidőben  
(azaz **hatékonyan**)  
megoldhatók

**P** <sup>?</sup> **= NP**

Problémák, melyek  
polinomidőben  
**ellenőrizhetők**: ha adott a  
probléma bemenetének egy  
potenciális  $M$  megoldása,  
akkor az **hatékonyan**  
**leellenőrizhető**, hogy  $M$   
**tényleg megoldás-e**

Miért NP? Mert ezek a  
problémák megoldhatóak  
polinomidőben  
**nemdeterminisztikusan**

# AZ A SEJTÉS, HOGY $P \neq NP$ :

Például a

## FAKTORIZÁCIÓ:

Adott egy  $N$  összetett szám

Számoljuk ki azon  $p, q$

számokat, melyekre  $N = p \cdot q$

NP-köztes

NP

NP-teljes

P

A legnehezebb problémák

NP-ben: nem ismert rájuk hatékony algoritmus (de nemdeterminisztikusan hatékonyan megoldhatók)

Például:

- SAT
- Hátizsák
- Hamilton-út
- ...

A hatékonyan megoldható problémák NP-ben

Például

- Gyorsrendezés
- Dijkstra algoritmus
- ...

# A HAMILTON-ÚT PROBLÉMA ALGORITMIKUS MEGOLDÁSA

- A feladat:
  - Adott egy  $G$  irányított gráf  $\{1, \dots, n\}$  csúcsokkal
  - Kérdés: Van-e  $G$ -ben **minden csúcsot pontosan egyszer** érintő út 1-ből  $n$ -be?
- Megoldás **algoritmikusan**:
  - Generáljuk a  $G$  összes  $n$ -hosszú  $p$  csúcssorozatát
  - Minden ilyen  $p$ -re ellenőrizzük, hogy
    - 1-gyel kezdődik és  $n$ -re végződik-e
    - minden csúcs egyszer fordul-e elő benne
    - a szomszédos elemei élt alkotnak-e  $G$ -ben
  - Ha van olyan  $p$  melyre mindez teljesül, akkor a kimenet: **igen**, egyébként: **nem**
  - **Időigény**:  $O(n^n)$  lépés
- Lehet gyorsítani, de várhatóan **nem lesz exponenciálisnál jobb!**

Mi a baj az exponenciális függvénnel?

Az, hogy nagyon **meredeken növekszik**

- Például:  $n = 100$  esetén (azaz 100 csúcsú gráfra) ez már  **$2^{100}$  lépést** jelent (rossz esetben)
- Ennyi lehetőséget egyenként végig nézni már **több évbe** telne a föld összes számítási kapacitásával is
- Itt már **Moore törvénye** sem segít számottevően

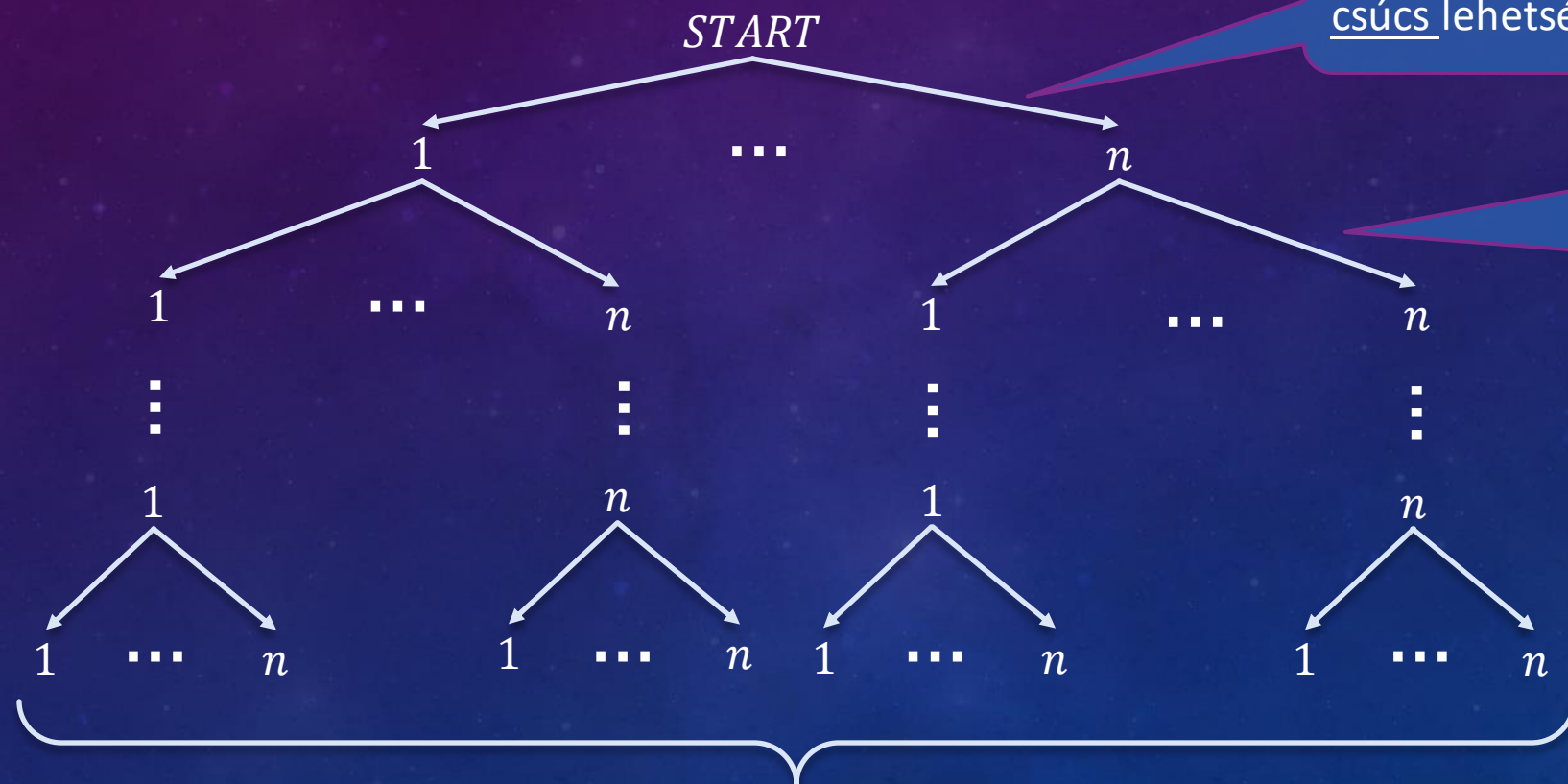
# A HAMILTON-ÚT PROBLÉMA NEMDETERMINISZTIKUS MEGOLDÁSA

Ez itt a nemdeterminizmus

- Generáljunk le  $G$  egy **tetszőleges**  $p$   $n$  hosszú csúcssorozatát (azaz állítsunk elő egy potenciális megoldást)
- Ellenőrizzük le, hogy  $p$  tényleg megoldás-e
  - 1-gyel kezdődik és  $n$ -re végződik-e
  - minden csúcs egyszer fordul-e elő benne
  - a szomszédos elemei élt alkotnak-e  $G$ -ben
- Ha tudunk így Hamilton-utat találni  $G$ -ben, akkor adjunk a kimenetre **igen** választ, egyébként pedig **nem**-et
- **Időigény**: annyi, mint a bekeretezett részé:  $O(n^2)$  lépés

# A HAMILTON-ÚT PROBLÉMA NEMDETERMINISZTIKUS MEGOLDÁSA

Tehát a **nemdeterminizmust** érdemes úgy felfogni, mint az összes potenciális megoldáson **párhuzamosan** futó számítást



$n$  párhuzamos számítás az első csúcs lehetséges értékeivel

$n^2$  párhuzamos számítás az első két csúcs lehetséges értékeivel

$n^n$  párhuzamos számítás az összes csúcs lehetséges értékeivel

# BIO-INSPIRÁLT SZÁMÍTÁSOK

A **természetben** is megfigyelhető **nagy fokú párhuzamosság**:

- Az élő sejtekben előforduló
  - nagy számú alkotórész
  - egyszerre (párhuzamosan) változik

Ezekkel vajon megoldhatók nehéz problémák hatékonyan?

Ezzel a kérdéssel foglalkozik a természet motiválta számítások közé tartozó

- **Membrán számítás** és
- **DNS számítás**

Alapötlet:

**TIME-SPACE TRADEOFF**

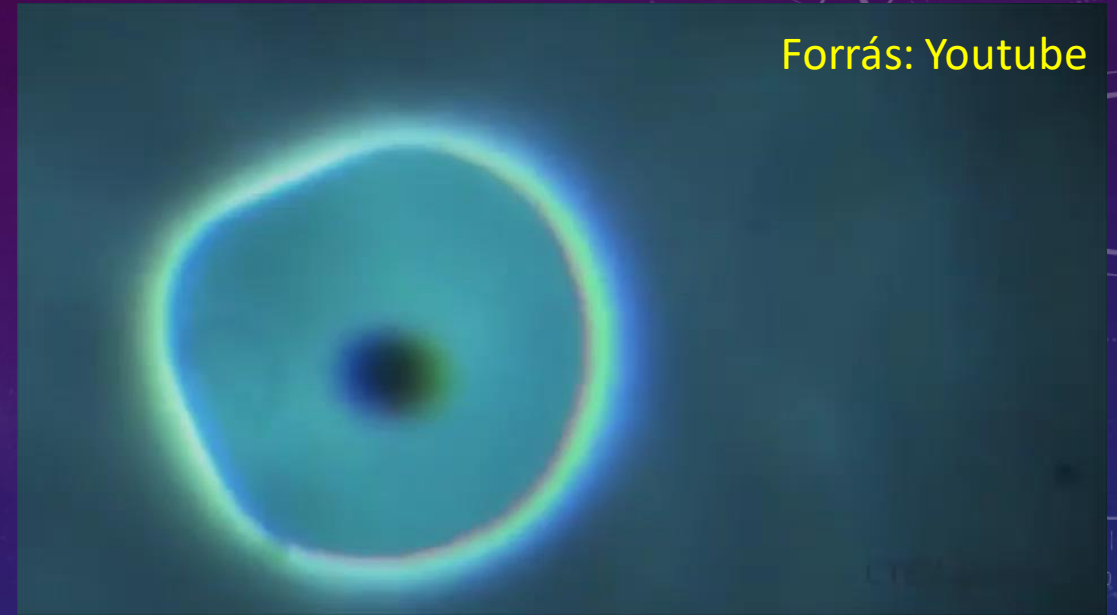
Mit jelent ez?

Ahelyett, hogy **kevés számítási** eszköz dolgozna **nem hatékonyan** dolgozzon **nagyon sok**, de egyszerű eszköz **hatékonyan!!!**

# MEMBRÁN ÉS DNS SZÁMÍTÁS

Hogyan készítsük el ezt az **nagyon sok** számítási eszközt?

A **DNS számítás**ban a láncok duplikálásával (PCR)



A **membrán számítás**ban a sejtek **osztódásával**

# KVANTUMSZÁMÍTÁS

A kvantummechanikában is megjelenik a **párhuzamosság**

Az alapgondolat:

## HASZNÁLJUNK KVANTUMBITET!!!

- Ez egy olyan **atomi eszköz** (pl. foton, elektron), melynek **két bázisállapota** (pl. polarizáció, spin) van
- Mindig a bázisállapotok szuperpozíciójában van:  $\alpha|0\rangle + \beta|1\rangle$
- 2 kvantumbitből álló rendszer leírásához már 4 szám kell
- ...
- $n$  kvantumbitből álló rendszer leírásához már  $2^n$  szám kell
- Azaz  $n$  kvantumbitből álló rendszer  $2^n$  számon tud egyszerre műveletet végezni!!!!

**Apró probléma:** méréskor egy ilyen rendszer beesik valamelyik bázisállapotába

**Megoldás:** kvantumalgoritmusok