

# Problémától a diszkrét modellig

## 5. óra: Hazudós barkóba, hibajavító kódok

Burcsi Péter

ELTE IK

2024-10-07

## Második témakör: keresés hibatűréssel

- Hazudós barkóba (Rényi–Ulam-játék)
- Csoporttesztelés
- Hibajavító kódok
- Kis információelmélet

- Hazudós barkóba konkrét példán
- Alsó becslés
- Hibajavító kódokkal való kapcsolat, Hamming-korlát
- Paraméterter mérése, stratégia a játékhoz

- Gondoltam egy számra 1 és 10 között, mi lehet az? Igen-nem kérdések
  - Hagyományos játék: legalább  $\log_2 N$  kérdés, ha 1 és  $N$  között
  - Akkor is, ha előre el kell küldeni a kérdéseket (adaptív / non-adaptív változat)?
- Most: a válaszadó hazudhat (legfeljebb egyszer)
- Kérdések: „Eleme-e a szám a  $H$  részhalmaznak?”
- Érvénytelen: „Hazudtál-e már?”
- Biztosan jó: 3-szor megkérdezek mindent
- Picit jobb: 2-szer kérdezek mindent, csak inkompatibilis válasznál kérdezek rá harmadszor

# Alsó becslés a kérdések számára

- Alsó becslés hagyományos barkóba esetén:
- Különböző szám  $\implies$  különböző válaszszorozat
- Ha  $n$  hosszú bináris sorozatok száma legalább  $N$ , akkor  $n \geq \log N$ 
  - Most: minden számra írjuk fel, mi lenne a HELYES válasz az  $n$  kérdésre.
  - Minden kapott sorozat különböző, SŐT:
  - Minden kapott sorozat eltér legalább 3 helyen
  - (Miért nem elég kettő helyen?)
- Hány ilyen sorozat lehetséges  $N = 10$  esetén?

# Hamming-korlát

- $n$  hosszú bitsorozatok
- Egy helyen elrontott (hazug) sorozatok is különbözők
- Egy igaz sorozathoz  $n$  hazug tartozik

$$(n + 1) \cdot 10 \leq 2^n$$

- $n \geq 7$
- Általánosan ( $t$  hazugságnál):

$$N \cdot \sum_{k=0}^t \binom{n}{k} \leq 2^n$$

# Hibajavító kódolás

- El kell küldenem egy üzenetet (pl. 1-től 10-ig egy szám),  $n$  bitet használhatok
- Az üzenet egy helyen megsérülhet, de még el akarjuk olvasni
- Általánosabban:  $t$  helyen sérülhet.
- Ehhez bármelyik két kódszó távolsága legyen  $2t + 1$  legalább

# Zárójel: négyelemű test

- Cél: három hosszúságú üzenet elküldése
- Plusz két betűt használhatunk
- Egy hibát ki kell tudni javítani
- Hamming-korlát: binárisan nem megy
- Modulo 5: rendben
- Modulo 4: elvileg működhetne, de nem megy lineárisan
- Négyelemű test: pont elég („tökéletes kód”)



# Vissza: barkóba hazugsággal

- Rögzítsük, hogy  $q$  kérdésünk van
- Hogy állunk, miután feltettünk pár kérdést?
  - Maradt még néhány kérdésünk
  - Életben maradt néhány szám
  - NAGYON életben maradt néhány szám
- Csak az a fontos, hogy melyikből mennyi:
- $x_0$  darab számhoz még nem kellett hazudni
- $x_1$  darab szám már csak akkor lehet, ha hazudtunk egyet
- Hogy mennyi munka van még hátra: SÚLY

$$w_q(x_0, x_1) = (q + 1) \cdot x_0 + x_1$$

- Mi történik a számokkal, ha választ kapunk egy új kérdésre:
- Az  $x_0$  szám közül mondjuk  $a_0$ -ra igaz
- Az  $x_1$  szám közül  $a_1$ -re.
- Igen válasz esetén az új helyzet:

$$(y_0, y_1) = (a_0, a_1 + (x_0 - a_0))$$

- Nem válasz esetén:

$$(z_0, z_1) = (x_0 - a_0, x_1 - a_1 + a_0)$$

- Mindenképpen teljesül (bármilyen  $a_0, a_1$  esetén:

$$w_q(x_0, x_1) = w_{q-1}(y_0, y_1) + w_{q-1}(z_0, z_1)$$

- Cél: lehető legjobb kérdést feltenni, ami (kb.) felezi a súlyt

# Stratégia, kis példával

- Mi legyen az első kérdés  $N = 10$  esetén?