

3. ZADATAK.

$$[0, \dots, m-1]$$

$$h: U \rightarrow [0, \dots, m-1]$$

$$m = 2^k$$

$$1) j = h(h), i = 0$$

2) TERMINIRAJ ako nađemo poziciju
ili je ona prazna

$$3) i++ \text{ , ako } i = m \text{ TERMINIRAJ}$$

$$\text{MAJE } j = (i+1) \% m \text{ NASTAVI}$$

NA 2. KORAK

4) Pokaži da je DANO PRETVAŽIVANJE instance

KVD, PROBLJEMO IJ. ODOBIO c_1, c_2

$$h(h, i) = (f(h) + c_1 i + c_2 i^2) \bmod m$$

$$h(h, 0) = j \quad j \bmod m$$

$$h(h, 1) = (j+1 + c_1 + c_2) \bmod m \quad (j+1) \bmod m$$

$$h(h, 2) = (j+2 + 2c_1 + 4c_2) \bmod m \quad (j+2) \bmod m$$

⋮

⋮

⋮

$$h(h, i) = (j+i + c_1 + c_2 i^2) \bmod m \quad (j+i) \bmod m$$

$$\Rightarrow h(h, i) = (f(h) + c_1 i + c_2 i^2) \bmod m$$

\Rightarrow Dano pretvaživanje je instance kvd. prob.

5) Pokažite da je ALG. PAK. PREMAZIO SVAKU POZICIJU u TABlici

Recimo da postoji pozicija j koju ne pretražujemo (algoritam neće doći do te pozicije)

1. SLUČ. Traženi ključ se nalazi na

poziciji j . Ključ neće biti promijenjen

jer se pretraga neće nastaviti

na novu poziciju j .

2. SLUČ. Traženi ključ se ne nalazi

na poziciji j , tj. algoritam će preći i

na novu poziciju j što znači da će pretražiti

i nje same iz čega slijedi kontradikcija

naše početne tvrdnje,

tj. sve pozicije će biti pretražene

$$m = 2^h \Rightarrow h(h, i) = (f(h) + c_1 i + c_2 i^2) \bmod 2^h = (j+i) \bmod 2^h$$

pošto vrijedi za $i \in [0, \dots, m-1]$ uzmemo

$$i = 0, i = 1$$

$$i = 0 \Rightarrow f(h) \bmod 2^h = j \bmod 2^h$$

$$\Rightarrow c_1 \text{ proizvoljan npr. } c_1 = 1$$

$$\Rightarrow (f(h) + c_1 + c_2) \bmod 2^h = (j+1) \bmod 2^h$$

$$= (j \bmod 2^h + 1) \bmod 2^h = (j \bmod 2^h - 1) \bmod 2^h$$

PRAKTIČNO:

$$= (f(h) + c_1 + c_2 - j - 2^h + 1) \bmod 2^h = 0$$

$$c_2 = j - f(h) - c_1 - 1 + 2^h$$

$$c_2 = (j - (j+1) \bmod 2^{h-1-1+2^h}) \bmod 2^h$$

$$c_2 = (2^h - 1) \bmod 2^h$$

$$c_2 = 1$$

$$\Rightarrow c_1 = c_2 = 1 //$$