

ZADACIA 1.

1.

1.a)

77, 69, 39, 70, 6, 8, 40, 89, 49, 15, $m = 19$

$$h(77) = 77 \bmod 19 = 1$$

$$h(69) = 69 \bmod 19 = 12$$

$$h(39) = 1$$

$$h(70) = 13$$

$$h(6) = 6$$

$$h(8) = 8$$

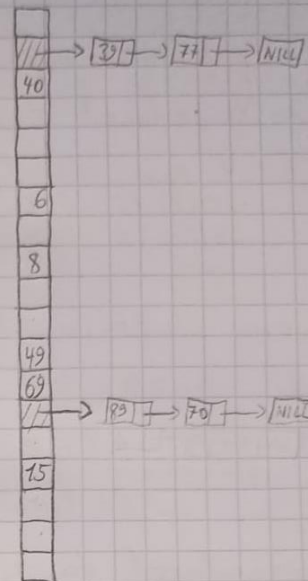
$$h(40) = 2$$

$$h(89) = 13$$

$$h(49) = 11$$

$$h(15) = 15$$

\Rightarrow



1.b)

$$h(77, 0) = (h_1(77) + 0 \cdot h_2(77)) \bmod 19 = 1$$

$$h(69, 0) = h_1(69) \bmod 19 = 12$$

$$h(39, 0) = h_1(39) \bmod 19 = 1$$

$$h(39, 1) = (h_1(39) + 1 \cdot h_2(39)) \bmod 19 = 5$$

$$h(70, 0) = h_1(70) \bmod 19 = 13$$

$$h(6, 0) = h_1(6) \bmod 19 = 6$$

$$h(8, 0) = h_1(8) \bmod 19 = 8$$

$$h(40, 0) = h_1(40) \bmod 19 = 2$$

$$h(89, 0) = h_1(89) \bmod 19 = 13$$

$$h(89, 1) = (h_1(89) + 1 \cdot h_2(89)) \bmod 19 = 11$$

$$h(89, 2) = (h_1(89) + 2 \cdot h_2(89)) \bmod 19 = 11$$

$$h(49, 0) = h_1(49) \bmod 19 = 11$$

$$h(49, 1) = (h_1(49) + 1 \cdot h_2(49)) \bmod 19 = 6$$

$$h(49, 2) = (h_1(49) + 2 \cdot h_2(49)) \bmod 19 = 1$$

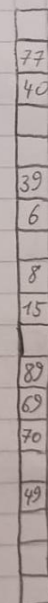
$$h(49, 3) = (h_1(49) + 3 \cdot h_2(49)) \bmod 19 = 15$$

$$h(15, 0) = h_1(15) \bmod 19 = 15$$

$$h(15, 1) = (h_1(15) + 1 \cdot h_2(15)) \bmod 19 = 12$$

$$h(15, 2) = (h_1(15) + 2 \cdot h_2(15)) \bmod 19 = 9$$

\Rightarrow



2.)

Da bi f-ja $f(x)$ bila univerzalna, mora zadovoljavati sljedeće uvjete:

1. Funkcija mora biti definirana za sve moguće ulaze x , tj. svi n -znamenasti decimalni brojevi s decimalnim znamenkama $\{0, 1, \dots, 9\}$.
2. Vrijednost f -je $f(x)$ moraju biti $\in \mathbb{Z}$
3. \forall par različitih ulaza x i y , vjerojatnost da će f-ja vratiti istu vrijednost za oba ulaza, tj. vjerojatnost kolizije, mora biti jednaka $1/m$, m - broj mogućih izlaza f-je

U ovom slučaju f-ja nije univerzalna jer za npr.:

$$n=2, a_1=a_2=1 \text{ i za npr. } 12 \text{ i } 83$$

$$\Rightarrow 1 \cdot 1 + 2 \cdot 1 = 3 \bmod 8 = 3$$

$$8 \cdot 1 + 3 \cdot 1 = 11 \bmod 8 = 3$$

Vjerojatnost da se preslikaju u isto je $> \frac{1}{8}$.

②

Ako definiramo slučajnu varijablu X koja modelira vjerojatnost kolizije za $0, \dots, n-1$ ključeva:

$$X \sim \begin{pmatrix} 0 & 1 & 2 & \dots & n-1 \\ 0 & \frac{1}{m} & \frac{2}{m} & \dots & \frac{n-1}{m} \end{pmatrix}$$

$$\Rightarrow EX = \sum_{i=1}^n \frac{n \cdot i}{m} = \frac{n^2 - n(n+1)}{2m} = \frac{n^2 - n}{2m} = \frac{1}{2} \cdot \frac{n(n-1)}{m}$$

Očekivani broj kolizija je proporcionalan broju ključeva kvadratno,

③.

1.) Za i -to ubacivanje ključa, vjerojatnost da zahtijeva strogo više od k probiranja jednaka je vjerojatnosti da prvih $k-1$ mjesta u tablici već bude zauzeto. Vjerojatnost da prvo mjesto bude zauzeto je n/m , drugo mjesto $(n-1)/(m-1)$ (jer se već zauzelo jedno mjesto), treće $(n-2)/(m-2)$, ... Stoga je vjerojatnost da zahtijeva više od k probiranja:

$$P\{X_i > k\} = \frac{n}{m} \cdot \frac{n-1}{m-1} \cdots \frac{n-k+1}{m-k+1}$$

Kako vrijedi $n \leq m/2$, za $k = \lceil \lg n \rceil$, dobivamo:

$$P\{X_i > \lceil \lg n \rceil\} \leq \frac{n}{m} \cdot \frac{n-1}{m-1} \cdots \frac{n - \lceil \lg n \rceil + 1}{m - \lceil \lg n \rceil + 1} \leq \frac{n}{m} \cdot \frac{n}{m} \cdots \frac{n}{m} = \dots$$

$$\dots = \left(\frac{n}{m}\right)^{\lceil \lg n \rceil} \leq 2^{-\frac{\lceil \lg n \rceil}{2}} \leq 2^{-\frac{k}{2}}$$

Ovdje smo koristili činjenicu da je umnožak manji od $\left(\frac{n}{m}\right)^k$ jer je svaki član umnoška $\leq \frac{n}{m}$.

2.) Vjerojatnost da i -to ubacivanje zahtijeva više od $2 \lg n$ probiranja je:

$$P \leq 2^{-2^{1/2} n} = 2^{-\frac{1}{2} n^{1/2}} = \frac{1}{n^{1/2}} \Rightarrow O\left(\frac{1}{n^{1/2}}\right)$$

3.) Ako je $X = \max\{X_i : 1 \leq i \leq n\}$,

$$\begin{aligned} P\{X > 2 \lg n\} &= P\{X_1 > 2 \lg n \vee X_2 > 2 \lg n \vee \dots \vee X_n > 2 \lg n\} = \\ &= \sum_{i=1}^n P\{X_i > 2 \lg n\} \leq \sum_{i=1}^n \frac{1}{n^{1/2}} = \frac{n}{n^{1/2}} = \frac{1}{n^{1/2}} \Rightarrow O\left(\frac{1}{n^{1/2}}\right) \end{aligned}$$

$$4.) EX = \sum_{i=1}^n i \cdot P\{X=i\} \leq P\{X \leq 2 \lg n\} 2 \lg n + P\{X > 2 \lg n\} n \leq \dots$$

$$\dots \leq \frac{n-1}{n} 2 \lg n + \frac{1}{n} \cdot n = 2 \lg n + 1 - \frac{2 \lg n}{n} \in O(\lg n)$$