Larisa Dragković

SPA II

ZADAĆA I.

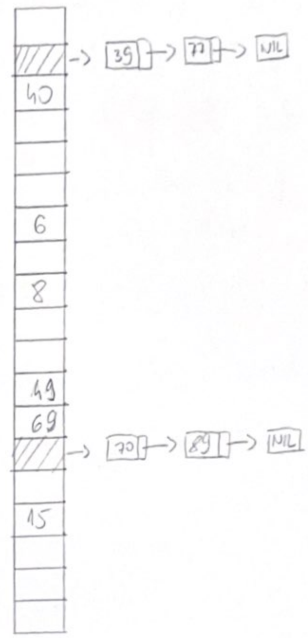
ZADATAK 1.

a) Demonstrirajte ubacivanje ključeva 77, 69, 39, 70, 6, 8, 40, 89, 49, 15 u hash tablicu veličine $m = 19$:

- u kojem se kolizije rješavaju ulančavanjem, gdje je dana funkcija raspršenja $h(k) = k \bmod m$

$h(k) = k \bmod m$

$h(77) = 77 \bmod 19 = 1$
$h(69) = 69 \bmod 19 = 12$
$h(39) = 39 \bmod 19 = 1$
$h(70) = 70 \bmod 19 = 13$
$h(6) = 6 \bmod 19 = 6$
$h(8) = 8 \bmod 19 = 8$
$h(40) = 40 \bmod 19 = 2$
$h(89) = 89 \bmod 19 = 13$
$h(49) = 49 \bmod 19 = 11$
$h(15) = 15 \bmod 19 = 15$



b) - u kojem se kolizije rješavaju probiranjem za $i = 0, 1, 2, \ldots, m-1$ koristeći dvostruko probiranje
$h(k,i) = (h_1(k) + i \cdot h_2(k)) \bmod m$, gdje su $h_1(k) = k \bmod m$, $h_2(k) = 1 + (k \bmod (m-1))$ pomoćne hash funkcije

$h(77,0) = (h_1(77) + 0 \cdot h_2(77)) \bmod 19 = 1$
$h(69,0) = (h_1(69) + 0 \cdot h_2(69)) \bmod 19 = 12$
$h(39,0) = (h_1(39) + 0 \cdot h_2(39)) \bmod 19 = 1$
$h(39,1) = (h_1(39) + 1 \cdot h_2(39)) \bmod 19 = 5$
$h(70,0) = (h_1(70) + 0 \cdot h_2(70)) \bmod 19 = 13$
$h(6,0) = (h_1(6) + 0 \cdot h_2(6)) \bmod 19 = 6$
$h(8,0) = (h_1(8) + 0 \cdot h_2(8)) \bmod 19 = 8$
$h(40,0) = (h_1(40) + 0 \cdot h_2(40)) \bmod 19 = 2$
$h(89,0) = (h_1(89) + 0 \cdot h_2(89)) \bmod 19 = 13$
$h(89,1) = (h_1(89) + 1 \cdot h_2(89)) \bmod 19 = 12$
$h(89,2) = (h_1(89) + 2 \cdot h_2(89)) \bmod 19 = 11$
$h(49,0) = (h_1(49) + 0 \cdot h_2(49)) \bmod 19 = 11$
$h(49,1) = (h_1(49) + 1 \cdot h_2(49)) \bmod 19 = 6$
$h(49,2) = (h_1(49) + 2 \cdot h_2(49)) \bmod 19 = 1$
$h(49,3) = (h_1(49) + 3 \cdot h_2(49)) \bmod 19 = 15$

$h(15,0) = (h_1(15) + 0 \cdot h_2(15)) \bmod 19 = 15$
$h(15,1) = (h_1(15) + 1 \cdot h_2(15)) \bmod 19 = 12$
$h(15,2) = (h_1(15) + 2 \cdot h_2(15)) \bmod 19 = 9$

ZADATAK 2. (ZADATAK 1. pod 2.)

Kako bi funkcija $f(x)$ bila univerzalna, ona treba zadovoljavati uvjete

1. Funkcija mora biti definirana za sve moguće ulaze X, to jest svi m-znamenkasti decimalni brojevi s decimalnim znamenkama $\{0, 1, \dots, 9\}$.
2. Vrijednost funkcije $f(x)$ mora biti element iz skupa cijelih brojeva
3. Za svaki par različitih ulaza x i y, vjerojatnost da će funkcija vratiti istu vrijednost za oba ulaza, to jest vjerojatnost kolizije, mora biti jednaka $\frac{1}{m}$; m je broj mogućih izlaza funkcije

- Funkcija nije univerzalna

pr. $m = 2$ $a_1 = a_2 = 1$ npr: 45 i 26

ZADATAK 2.

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

$$X \sim \begin{pmatrix} 0 & 1 & 2 & 3 & & m-1 \\ 0 & \frac{1}{m} & \frac{2}{m} & \frac{3}{m} & \dots & \frac{m-1}{m} \end{pmatrix}$$

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

Očekivani broj kolizija je kvadratno proporcionalan broju ključeva

Larisa Darojković

ZADATAK 3.

1.) Za ito ubacivanje ključa, vjerojatnost da zahtjeva 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 $\frac{n}{m}$, drugo mjesto $\frac{(n-1)}{(m-1)}$ jer je već zauzeto jedno mjesto, treće $(n-1)(m-2)$,... stoga je vjerojatnost da zahtjeva 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 $n \leq \frac{m}{2}$, za $k = \lfloor \lg m \rfloor$ dobit ćemo:

$$P\{X_i > \lfloor \lg m \rfloor\} \leq \frac{n}{m} \cdot \frac{n-1}{m-1} \cdots \frac{n-\lfloor \lg m \rfloor+1}{m-\lfloor \lg m \rfloor+1} \leq \frac{n}{m} \cdot \frac{n}{m} \cdots \frac{n}{m} = \ldots =$$

$$= \left(\frac{n}{m}\right)^{\lfloor \lg m \rfloor} \leq 2^{-\frac{\lfloor \lg m \rfloor}{2}} \leq 2^{\frac{-k}{2}}$$

- umnožak manji od $\left(\frac{n}{m}\right)^k$ jer je svaki član umnoška manji ili jednak $\frac{n}{m}$

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

$$\leq 2^{-2\lg m} = 2^{\lg m^{-2}} = \frac{1}{m^2} \Rightarrow O\left(\frac{1}{m^2}\right).$$

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

$$P\{X > 2\lg m\} = P\{X_1 > 2\lg m \lor X_2 > 2\lg m \lor \ldots \lor X_n > 2\lg m\}$$

$$= \sum_{i=1}^{n} P\{X_i > 2\lg m\} \leq \sum_{i=1}^{n} \frac{1}{m^2} = \frac{n}{m^2} = \frac{1}{m} \Rightarrow O\left(\frac{1}{m}\right)$$

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

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