ZADATAK 1.

Domaća 1.

1

a) $h(k) = k \bmod m$, $m = 19$

$h(77) = 1$

$h(69) = 12$

$h(39) = 1$

$h(70) = 13$

$h(6) = 6$

$h(8) = 8$

$h(40) = 2$

$h(89) = 13$

$h(49) = 11$

$h(15) = 15$

0		
1		→ 77 → 39
2	40	
3		
4		
5		
6	6	
7		
8	8	
9		
10		
11	49	
12	69	
13		→ 70 → 89
14		
15	15	
16		
17		
18		

b) $h(k,i) = (h_1(k) + i \cdot h_2(k)) \bmod m$, $m = 19$

$h_1(k) = k \bmod m$ $\quad$ $h_2(k) = 1 + (k \bmod (m-1))$

0	
1	77
2	40
3	
4	
5	39
6	6
7	
8	8
9	15
10	
11	89
12	69
13	70
14	
15	49
16	
17	
18	

KEY = 77

$h_1(77) = 1$

$h_2(77) = 6$

$h(77,0) = (1 + 0 \cdot 6) \bmod 19$

$\boxed{h(77,0) = 1}$ ✓ SLOBODNO

KEY = 39

$h_1(39) = 1$

$h_2(39) = 4$

$h(39,0) = (1 + 0 \cdot 4) \bmod 19$

$h(39,0) = 1$ ✗ ZAUZETO

$h(39,1) = (1 + 1 \cdot 4) \bmod 19$

$\boxed{h(39,1) = 5}$ ✓ SLOBODNO

KEY = 6

$h_1(6) = 6$

$h_2(6) = 7$

$h(6,0) = (6 + 0 \cdot 7) \bmod 19$

$\boxed{h(6,0) = 6}$ ✓ SLOBODNO

KEY = 69

$h_1(69) = 12$

$h(69) = 16$

$h(69,0) = (12 + 0 \cdot 16) \bmod 19$

$\boxed{h(69,0) = 12}$ SLOBODNO ✓

KEY = 70

$h_1(70) = 13$

$h_2(70) = 17$

$h(70,0) = (13 + 0 \cdot 17) \bmod 19$

$\boxed{h(70,0) = 13}$ ✓ SLOBODNO

KEY = 8

$h_1(8) = 8$

$h_2(8) = 9$

$h(8,0) = (8 + 0 \cdot 9) \bmod 19$

$\boxed{h(8,0) = 8}$ ✓ SLOBODNO

KEY = 40

$h_1(40) = 2$

$h_2(40) = 5$

$h(40,0) = (2 + 0 \cdot 5) \bmod 19$

$\boxed{h(40,0) = 2}$ ✓ SLOBODNO

KEY = 89

$h_1(89) = 13$

$h_2(89) = 18$

$h(89,0) = (13 + 0 \cdot 18) \bmod 19$

$h(89,0) = 13$ × ZAUZETO

$h(89,1) = (13 + 1 \cdot 18) \bmod 19$

$h(89,1) = 12$ × ZAUZETO

$h(89,2) = (13 + 2 \cdot 18) \bmod 19$

$\boxed{h(89,2) = 11}$ ✓ SLOBODNO

KEY = 49

$h_1(49) = 11$

$h_2(49) = 14$

$h(49,0) = (11 + 0 \cdot 14) \bmod 19$

$h(49,0) = 11$ × ZAUZETO

$h(49,1) = (11 + 1 \cdot 14) \bmod 19$

$h(49,1) = 6$ × ZAUZETO

$h(49,2) = (11 + 2 \cdot 14) \bmod 19$

$h(49,2) = 1$ × ZAUZETO

$h(49,3) = (11 + 3 \cdot 14) \bmod 19$

$\boxed{h(49,3) = 15}$ ✓ SLOBODNO

KEY = 15

$h_1(15) = 15$

$h_2(15) = 16$

$h(15,0) = (15 + 0 \cdot 16) \bmod 19$

$h(15,0) = 15$ × ZAUZETO

$h(15,1) = (15 + 1 \cdot 16) \bmod 19$

$h(15,1) = 12$ × ZAUZETO

$h(15,2) = (15 + 2 \cdot 16) \bmod 19$

$\boxed{h(15,2) = 9}$ ✓ SLOBODNO

2. Hash f-ja nije univerzalna

Da bi hash f-ja bila univerzalna mora vrijediti da je nasumično ulazne podatke, vjerojatnost da je njihov hash isti je moguća $\frac{1}{m}$.

UKUPAN BROJ MOGUĆIH HASH VRIJEDNOSTI

Kontraprimjer: $m = 2$, $a_1 = a_2 = 1$, $x = 0$, $y = 8$. Takva hash f-ja daje isti rezultat.

$$\left.\begin{aligned} f(x) &= 4 \cdot 1 + 4 \cdot 1 = 8 \bmod 8 = 0 \\ f(y) &= 9 \cdot 1 + 7 \cdot 1 = 16 \bmod 8 = 0 \end{aligned}\right\} 1 > \frac{1}{8}$$

VJEROJATNOST DA SE PRESLIKA

ZADATAK 2.

Hashiranje je uniformno što znači da vjerojatnost da neki ključ bude dodijeljen određenom polju je $\frac{1}{m}$.

I_{ij} nam je ključ i-ti, a I_{ij} nam je indikator i-te sl. varijable. $I_{ij} = \begin{cases} 1/m, & k(i) = k(j) \\ NULL, & inače \end{cases}$

Zbog uniformnosti vrijedi $E[I_{ij}] = \frac{1}{m}$. Zbog toga očekivani broj kolizija jednak je

$$E\left[\sum_{i=1}^{m} \sum_{j=1}^{m} I_{ij}\right] = \sum_{(\neq)} E[I_{ij}] = \sum_{(\neq)} \frac{1}{m} = \binom{m}{2} \frac{1}{m} = \frac{m(m-1)}{2m}$$

2 ključa od njih m

ZADATAK 3.

1. Neka je X_k slučajna varijabla koja predstavlja broj probanja u neuspješnom pretraživanju. Neka je A_k događaj $(k = 1, 2, \ldots, m)$ koji predstavlja k-ti probe i to mjesto je već zauzeto. Tada događaj $\{X_k > k\}$ je presjek događaja $A_1 \cap A_2 \cap \ldots \cap A_k$. Po uvjetnoj vjerojatnosti vrijedi

$$P_r\{A_1 \cap A_2 \cap A_3 \cap \ldots \cap A_k\} = P_r\{A_1\} \cdot P_r\{A_2 | A_1\} \cdot P_r\{A_3 | A_1 \cap A_2\} \cdot \ldots \cdot P_r\{A_k | A_1 \cap A_2 \ldots A_{k-1}\}$$

Za $j > 1$ vjerojatnost da je proba završila na zauzetom mjestu, uzimajući u obzir da su prvih $j-1$ probanja bila na zauzetim mjestima je $\frac{m-j+1}{m-j+1}$. $m-j+1$ predstavlja broj praznih slotova koji nisu pretraženi, a $m-j+1$ je ukupan broj preostalih slotova.

$$P_r\{X_k \geq k\} = \frac{m}{m}\cdot\frac{m-1}{m-1}\cdot\frac{m-2}{m-2}\cdot\frac{m-3}{m-3}\cdots\frac{m-k+1}{m-k+1} \leq \left(\frac{m}{m}\right)^k = \left(\frac{\frac{m}{2}}{m}\right)^k = \left(\frac{1}{2}\right)^k = 2$$

2. Postavimo ne na prijašnji dokaz, koristimo slučajnu varijablu X_k kao $X_{2\lg m}$. Tada imamo

$$P_r\{X_{2\lg m} \geq k\} = \frac{m}{m}\cdot\frac{m-1}{m-1}\cdot\frac{m-2}{m-2}\cdots\frac{m-2\lg m+1}{m-2\lg m+1}$$

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

3. U prethodnom dokazu smo pokazali za jedan insert, a kako pokazujemo sjedinjenu vjerojatnost, to je vjerojatnost maksimalnog broja probanja za bilo koji od m inserta. Znamo da i-ti insert ima je vjerojatnost $\frac{1}{m^2}$. Sjedinjenu vjerojatnost možemo računati kao događaja. Sumiramo jer imamo je obrnuto i to sve kojem je dobar jednako, dokaz kojim će može biti $O(\frac{1}{m})$.

$$P_r\{X_1 \geq 2\lg m\} + P_r\{X_2 \geq 2\lg m\} + P_r\{X_3 \geq 2\lg m\} + \ldots + P_r\{X_m \geq 2\lg m\}$$

$$= \sum_{i=1}^{m} P_r\{X_i \geq 2\lg m\} \leq \sum_{i=1}^{m} \frac{1}{m^2} = \frac{1}{m^2}\cdot m = \frac{1}{m}$$

4. Najduži mogući prolaz pretraživanja je m i iz prethodnog zadatka znamo da je vjerojatnost duljine veće od $2\lg m$ jednaka $\frac{1}{m}$. Imamo:

$$\Pr\{X \leq 2\lg m\} + P\{X > 2\lg m\} = 1$$

$$\Rightarrow E[X] \leq \Pr\{X \leq 2\lg m\} \cdot 2\lg m + P\{X > 2\lg m\} \cdot m$$

$$= \frac{m-1}{m} \cdot 2\lg m + \frac{1}{m} \cdot m = \frac{2\lg m \cdot m}{m} - \frac{2\lg m}{m} + 1 = 2\lg m - \frac{2\lg m}{m} + 1$$

$$= O(\lg m)$$