TECHNICKÁ UNIVERZITA V KOŠICIACH
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

25. HASH
Zadanie z predmetu MTaS

2018 **Martin Chlebovec**

Obsah

1. Popis problému

25. Hash funkcia

Vytvorte tabuľku vlastného profilu podľa predlohy:

N	Hodnoty	Vlastný profil	Váha	Hash
0	Meno	Jozef	000	
1	Práca	Tuke	001	
2	Adresa domov	Nad Jazerom	010	
3	Adresa práca	B.N. 32	011	
4	Obchod 1	Aupark	100	
5	Obchod 2	Optima	101	
6	Č. linky -> práca	9	110	
7	ID zariadenia	908 666 111	111	

Následne vytvorte ďalších 5 podobných tabuliek. V každej tabuľke potom údaje zo stĺpca N a Vlastný profil zakódujte Hashovacou funkciou. Následne porovnajte tabuľku s vlastným profilom s ostatnými tabuľkami. Porovnávať môžete len Hashované hodnoty. Z výsledkov porovnania vypočítajte percentuálnu zhodu profilov použitím váh.

1. Programové riešenie zadania

Zadanie som programovo riešil v prostredí MATLAB 2016b. Pri riešení úlohy Hash som sa musel v prvom rade zoznámiť s dostupnými hashovacími funkciami, ktoré prostredie podporuje. Bol som prekvapený, nakoľko MATLAB podporuje svoje hashovacie funkcie a aj funkcie príbuzných programovacích jazykov. Mal som na výber zo vstavaných - systémových knižníc, alebo knižníc jazyka Java, prípadne .NET.

Rozhodol som sa využiť systémovú knižnicu s hashovacou funkciou SHA1, ktorá dokáže

vygenerovať hash z ľubovoľného textového reťazca s fixnou dĺžkou, 20 bajtov pri HEX reprezentácii. Pri návrhu programu som využil aj študijné materiály z minulého roka z predmetu Úvod do digitálnych komunikácii, na ktorý predmet Mobilné technológie a služby nadväzuje.

```
close all;
clear all;
shalhasher = System.Security.Cryptography.SHA1Managed;
N = [0;1;2;3;4;5;6;7];
Hodnoty = {'Meno';'Práca';'Adresa domov';'Adresa práca';'Obchod 1';'Obchod 2';'Č linky
%UDAJE TABUIEK
Vlastny_profil = {'Martin';'Tuke';'Nad Jazerom';'BN32';'Optima';'Cassovia';'10';'119'};
Profil1 = {'Marek';'Tuke';'SNP';'BN 8';'Optima';'Billa';'R4';'52899'};
Profil2 = {'Alexander';'Optima';'Námestie osloboditeIov';'Timkovičová';'Lidl';'Cassovia
Profil3 = {'Tomáš';'UPJŠ';'Idanská';'Nová Nemocnica 1';'Optima';'Kaufland';'17';'18949'
Profil4 = {'Kristian';'Tuke';'Zimná';'Letná 9';'1-day';'Fresh';'9';'19987498'};
Profil5 = {'Jan';'USS';'Amfiteáter';'Štúrova 18';'COOP';'Sintra';'6';'61588'};
%KONIEC UDAJOV TABULIEK
%KONSTANTY
Vaha = {'000';'001';'010';'011';'100';'101';'110';'111'};
menol = char(Vlastny_profil(1));


%ZACIATOK MIEN
profmenol = char(Profil1(1));
profmeno2 = char(Profil2(1));
profmeno3 = char(Profil3(1));
profmeno4 = char(Profil4(1));
profmeno5 = char(Profil5(1));

%ZACIATOK PRAC
pracal = char(Vlastny_profil(2));
profpracal = char(Profil1(2));
profpraca2 = char(Profil2(2));
```

Využil som jednorozmerné polia textových reťazcov, ktorými som reprezentoval údaje tabuliek pre moje dáta a iné pre 5 tabuliek. Pri riešení úlohy som už v tomto bode narazil na prvý problém. Textový reťazec nebolo možné použiť v hashovacej funkcii, ktorá striktne žiadala premennú typu char, preto som premenné musel pretypovať pred predaním hashovacej funkcii.

```
%ZACIATOK ID
idl = char(Vlastny_profil(8));
profidl = char(Profil1(8));
profid2 = char(Profil2(8));
profid3 = char(Profil3(8));
profid4 = char(Profil4(8));
profid5 = char(Profil5(8));

%HASH MENO
shalmenol= uint8(shalhasher.ComputeHash(uint8(menol)));
menolshal = reshape(dec2hex(shalmenol),1,[]);
```

Výsledkom hashovacej funkcie bola dvojstĺpcová matica s desiatkovými číslami reprezentácie, pre lepšiu čitateľnosť som vykonal konverziu decimálnych čísel na hexadecimálne a previedol ich funkciou reshape na jednoriadkovú maticu. Tieto údaje som reprezentoval aj do výpisu programového okna MATLAB-u. Ďalším krokom bolo porovnanie hashovacích hodnôt.

T =

N	Hodnoty	Vlastny_profil	Vaha	Hash
0	'Meno'	'Martin'	'000'	'74F38C2E8FC0B0E1B53637DB65B233AB6A9AEF09'
1	'Práca'	'Tuke'	'001'	'969424397949CA09983AA8EBFCDD309C57800F70'
2	'Adresa domov'	'Nad Jazerom'	'010'	'68FE8CACF24F4F9FD8590E2CEC4B5169D34FD1A4'
3	'Adresa práca'	'BN32'	'011'	'A3427ECAC69FD5C6455F371BD82C32AA907DC633'
4	'Obchod 1'	'Optima'	'100'	'D1D7C5047DDA0A1DD26DF4DE7ED927462E4002C2'
5	'Obchod 2'	'Cassovia'	'101'	'EA0FE3E3DC70911CFF2C81D3F17F518D1FAC0102'
6	'Č linky -> práca'	'10'	'110'	'BD711D473E505E95C78E158118FBF4A82578DA75'
7	'ID zariadenia'	'119'	'111'	'AE334221048FACA86AB723D4F7E0DAEEB7EA08AA'

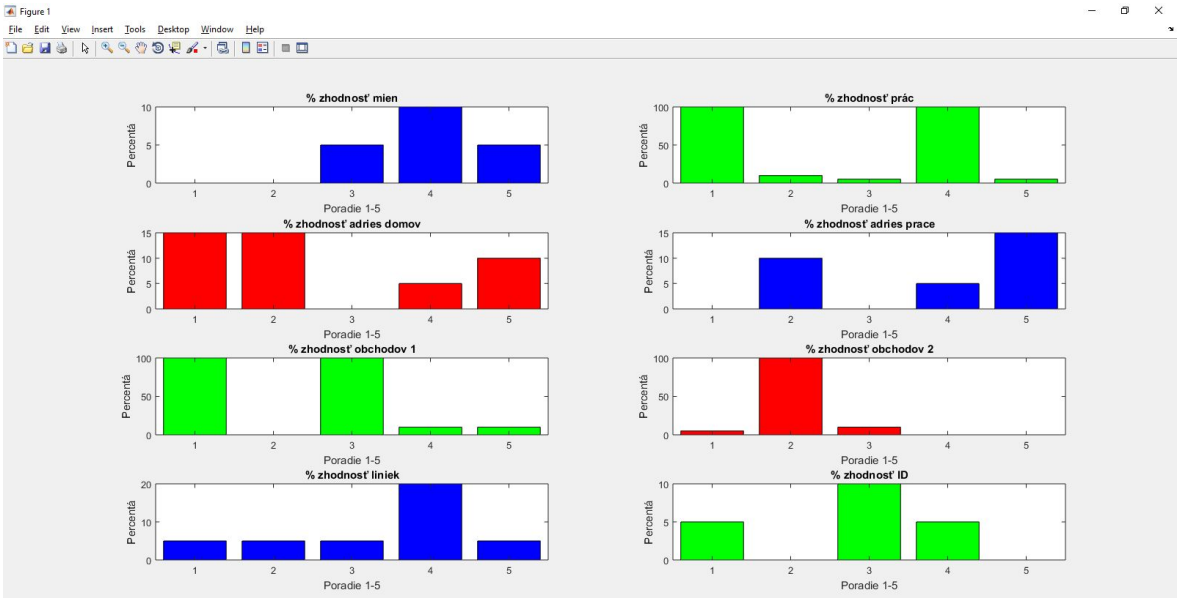
T1 =

N	Hodnoty	Profil1	Vaha	Hash1
0	'Meno'	'Marek'	'000'	'603BF7923E8AC56469955E0B0A7997553DF85087'
1	'Práca'	'Tuke'	'001'	'969424397949CA09983AA8EBFCDD309C57800F70'
2	'Adresa domov'	'SNP'	'010'	'B1348131F9F8B3DF8FCE1AFDFFC7D81C8764E33F'
3	'Adresa práca'	'BN 8'	'011'	'D07B3F2BBEDCA757EF43BA2363660EE2451E7A32'
4	'Obchod 1'	'Optima'	'100'	'D1D7C5047DDA0A1DD26DF4DE7ED927462E4002C2'
5	'Obchod 2'	'Billa'	'101'	'A2CF080F0F223E0463E1934BAA74A65DCB40EDD4'
6	'Č linky -> práca'	'R4'	'110'	'977761FE967E9D6D02C32199A5FCB31E5CFFB262'
7	'ID zariadenia'	'52899'	'111'	'B4D38CFA52FE528A593DFCFC466259949489FE49'

Riešenie rozdielu, alebo zhodnosti hashov som vyriešil porovnávaním znakov pod sebou medzi jednotlivými hashmi. Porovnával som môj profil a ostatných 5 profilov voči nemu. Výsledkom bola matica núl a jednotiek podľa zhodnosti jednotlivých znakov.

```
for linky = 1:20
    linky1(linky) =   strcmp(linka1sha1(linky),proflinka1sha1(linky));
    linky2(linky) =   strcmp(linka1sha1(linky),proflinka2sha1(linky));
    linky3(linky) =   strcmp(linka1sha1(linky),proflinka3sha1(linky));
    linky4(linky) =   strcmp(linka1sha1(linky),proflinka4sha1(linky));
    linky5(linky) =   strcmp(linka1sha1(linky),proflinka5sha1(linky));
end
```

Nakoľko som pre percentuálne vyjadrenie nevedel použiť systém váh, využil som sčítanie kladných bitov 20-bitovej postupnosti a tú som vydelil postupnosťou a výsledok násobil číslom 100. Výsledkom je percentuálna zhodnosť každej položky profilov medzi mojím a každým z piatich pre každú údaj. Výsledky s percentuálnym vyjadrením sú dostupné aj v grafickej podobe v grafoch, ktoré vizualizujú jednotlivé výsledky.



Záver a zhodnotenie zadania

Cieľom tejto práce bolo naučiť sa používať hashovaciu funkciu, pracovať s bitovou postupnosťou, využívať konverziu medzi sústavami, pretypovanie premenných, generovať grafické vyjadrenie údajov, percentuálne porovnať ľubovoľné reťazce, využívať pretváranie matíc. Riešenie sa mi nepodarilo zrealizovať predpísaným systémom váh, ale alternatívou som dosiahol uspokojivé výsledky, ktoré plnohodnotne reprezentujú percentuálne porovnanie hashovacích reťazcov. Moje riešenie v prostredí MATLAB má približne 500 riadkov kódu.