VŠB – TUO Datum _____

Teorie grafů

Projekt

číslo zadání ____

Osobní číslo _____ Jméno _____

Zadání

Sejf se otvírá digitální klávesnicí, přičemž sejf se otevře při zadání správné posloupnosti bez ohledu na předchozí stisknuté klávesy. Je-li například 1234 *heslo otvírající sejf, tak pro otevření můžeme zadat* **1234***, nebo* 8**1234** *nebo klidně* 6382543**1234**.

K prolomení kódu můžeme postupně zadat všechna čísla od 0000 *do* 9999*. Avšak to bychom museli naťukat celkem* $4 \cdot 10000 = 40000$ *cifer, což by trvalo zbytečně dlouho.*

a) Jaký je nejmenší počet cifer, který zajistí prolomení kódu?

b) Jak sestrojit příslušnou posloupnost čísel?

c) Uměli byste úlohu vyřešit i pro n*-ciferná čísla s číslicemi* $1, 2, \ldots, q$*?*

Řešení

Horní odhad nejmenšího počtu cifer je $4 \cdot 10000 = 40000$, avšak dolní odhad je pouhých 10 003 znaků (v posloupnosti $10000 + 3$ znaků najdeme 10000 po sobě jdoucích čtveřic). Nejprve ukážeme, že dolního odhadu je možno vždy dosáhnout a pak řešení zobecníme pro n-ciferná q-ární čísla.

Existenční důkaz
Úlohu převedeme na hledání eulerovského tahu v orientovaném grafu $D(V, E)$, kde

$$V = \{xyz : x, y, z \in \{0, 1, \ldots, 9\}\}, \quad E = \{(xyz, yzw) : xyz, yzw \in V\}.$$

Dva vrcholy jsou spojené hranou, jestliže se shodují poslední dvě cifry výchozího vrcholu a první dvě cifry koncového vrcholu. Každá hrana (včetně smyček) odpovídá jednomu čtyřcifernému číslu $xyzw$. V grafu D má každý vrchol xyz příchozí i odchozí stupeň $q = 10$.

$$\forall v \in V : \ \mathrm{ideg}(v) = \mathrm{odeg}(v) = q = 10.$$

Počet hran je

$$|E| = \frac{1}{2} \cdot |V| \cdot (\mathrm{ideg}(v) + \mathrm{odeg}(v)) = \frac{1}{2} \cdot 1000 \cdot (10 + 10) = 10000.$$

Protože je pro každý vrchol souvislého orientovaného grafu D platí $\mathrm{ideg}(v) = \mathrm{odeg}(v)$, tak podle známé Eulerovy věty existuje v D dokonce *uzavřený eulerovský tah*, který odpovídá hledané posloupnosti cifer. Pokud nás zajímá posloupnost čísel a ne jen uzavřený tah, musíme nejprve nějaký uzavřený tah najít, zvolit jeden vrchol a posloupnost sestavit:

1. jméno prvního vrcholu xyz jsou první tři znaky posloupnosti,
2. za každou hranu tahu přidáme jeden znak w – poslední znak koncového vrcholu hrany,
3. nakonec zopakujeme první tři znaky xyz.

Celkem dostaneme, že nejmenší počet cifer, který zajistí prolomení kódu, je právě 10 003 cifer.

Obecnější řešení
Úlohu převedeme na hledání eulerovského tahu v orientovaném grafu $D(V, E)$, kde vrcholy jsou posloupnosti $k - 1$ cifer

$$V = \{x_1 x_2 \ldots x_{k-1}) : x_i \in \{0, 1, \ldots, q\} \text{ pro } i = 1, 2, \ldots, k - 1\}$$

$$E = \{(x_1 x_2 \ldots x_{k-1}, x_2 x_3 \ldots x_k) : x_1 x_2 \ldots x_{k-1}, x_2 x_3 \ldots x_k \in V\}.$$

Dva vrcholy jsou spojené hranou, jestliže se shoduje posledních $k-2$ cifer výchozího vrcholu a $k-2$ prvních cifer koncového vrcholu. Každá hrana (včetně smyček) odpovídá jednomu k-ciferném číslu. V grafu D má každý vrchol v příchozí i odchozí stupeň q.

$$\forall v \in V : \ \mathrm{ideg}(v) = \mathrm{odeg}(v) = q.$$

Počet hran je

$$|E| = \frac{1}{2} \cdot |V| \cdot (\mathrm{ideg}(v) + \mathrm{odeg}(v)) = \frac{1}{2} \cdot q^{n-1} \cdot (q+q) = \frac{1}{2} \cdot q^{n-1} \cdot 2q = q^n.$$

Protože je pro každý vrchol orientovaného grafu D platí $\mathrm{ideg}(v) = \mathrm{odeg}(v) = q$ a D je určitě souvislý, tak podle známé Eulerovy věty existuje v D dokonce *uzavřený eulerovský tah*, který odpovídá hledané posloupnosti cifer. Opět, pokud nás zajímá posloupnost čísel a ne uzavřený cyklus, musíme nějaký uzavřený tah najít a posloupnost zkonstruovat:

1. zvolíme jeden vrchol a jeho jméno je prvních $n-1$ znaků posloupnosti,
2. za každou hranu tahu přidáme jeden znak w – poslední znak koncového vrcholu hrany,
3. nakonec zopakujeme prvních $n-1$ znaků.

Nejmenší počet cifer, který zajistí prolomení kódu, je právě $q^n + n - 1$ cifer.

Více informací je možno najít pod klíčovým slovem „de Bruijn“, nebo „debruijn“.

Shrnutí

a) Ukázali jsme, že nejmenší počet cifer, který zajistí prolomení kódu, je právě 10 003 cifer.

b) Příslušnou posloupnost sestrojíme nalezením eulerovského tahu v pravidelném orientovaném grafu $D(V, E)$, který je popsaný výše.

c) Nakonec jsme úlohu zobecnili pro libovolná n-ciferná čísla s číslicemi $1, 2, \ldots, q$. Nejmenší počet cifer, který zajistí prolomení kódu, je $q^n + n - 1$.