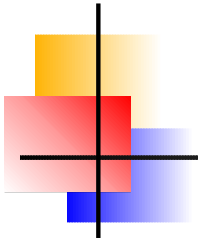
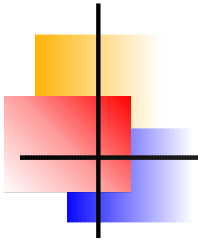


Objavovanie a opravovanie chýb

Stanislav Palúch

Fakulta riadenia a informatiky, Žilinská univerzita

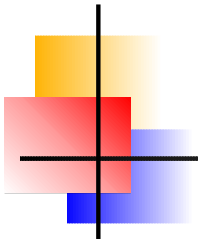
21. apríla 2021



Najčastejšie chyby pri písaní na klávesnici

Z anglosaskej literatúry máme údaje o relatívnej početnosti chýb vznikajúcich písaním textov na klávesnici resp. písacom stroji.

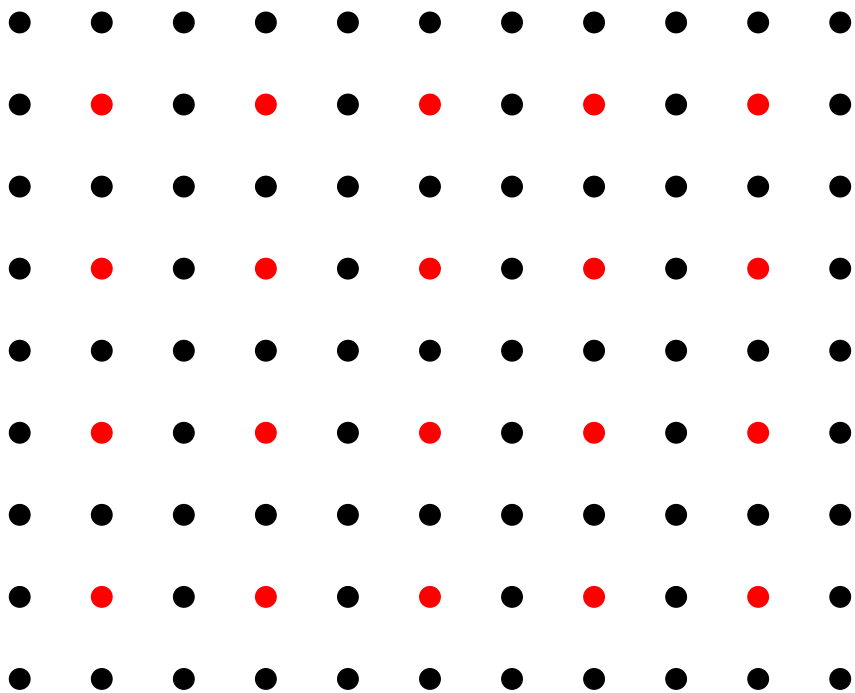
- Jednoduchá chyba $a \to b$ 79%
- Susedná transpozícia $ab \to ba$ 10.2%
- Skoková transpozícia $abc \to cba$ 0.8%
- Blíženci $aa \to bb$ 0.6%
- Fonetická chyba $X0 \to 1X$ 0.5%
- Ostatné chyby 8.9%

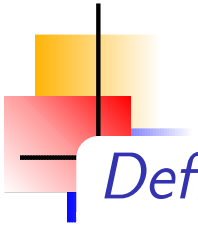


Všeobecný princíp objavovania chýb

Len niektoré slová z A^n budú kódové, osatné slová nekódové.

Ak prijmeme nekódové slovo, vieme že nastala pri prenose chyba.





Metrika na množine slov

Definícia

Reálna funkcia d definovaná na karteziánskom súčine $V \times V$ sa nazýva **metrikou na množine** *V, ak platí:*

1. *Pre každé $u, v \in V$ je $d(u, v) \geq 0$*
   a rovnosť nastáva práve vtedy, keď $u = v$.
2. *Pre každé $u, v \in V$ je $d(u, v) = d(v, u)$.*
3. *Ak $u, v, w \in V$, potom $d(u, w) \leq d(u, v) + d(v, w)$.*

Definícia

Hammingova vzdialenosť *$d(\mathbf{v}, \mathbf{w})$ dvoch slov $\mathbf{v} = v_1 v_2 \ldots v_n$, $\mathbf{w} = w_1 w_1 \ldots w_n$ je počet miest, na ktorých sa znaky slov $\mathbf{v}$, $\mathbf{w}$ líšia, t. j.*

$$d(\mathbf{v}, \mathbf{w}) = \left|\{i \mid v_i \neq w_i, \quad i = 1, 2, \ldots, n\}\right|.$$

Ľahko sa dá ukázať, že Hammingova vzdialenosť má vlastnosti metriky, a preto sa niekedy volá aj **Hammingova metrika**.

Metrika na množine slov

Definícia

Reálna funkcia d definovaná na karteziánskom súčine $V \times V$ sa nazýva **metrikou na množine** *V, ak platí:*

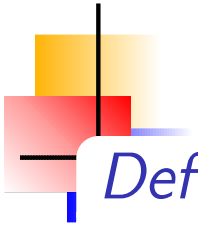
1. *Pre každé $u, v \in V$ je $d(u, v) \geq 0$*
   a rovnosť nastáva práve vtedy, keď $u = v$.
2. *Pre každé $u, v \in V$ je $d(u, v) = d(v, u)$.*
3. *Ak $u, v, w \in V$, potom $d(u, w) \leq d(u, v) + d(v, w)$.*

Definícia

Hammingova vzdialenosť *$d(\mathbf{v}, \mathbf{w})$ dvoch slov $\mathbf{v} = v_1 v_2 \ldots v_n$, $\mathbf{w} = w_1 w_1 \ldots w_n$ je počet miest, na ktorých sa znaky slov $\mathbf{v}$, $\mathbf{w}$ líšia, t. j.*

$$d(\mathbf{v}, \mathbf{w}) = \left|\{i \mid v_i \neq w_i, \quad i = 1, 2, \ldots, n\}\right|.$$

Ľahko sa dá ukázať, že Hammingova vzdialenosť má vlastnosti metriky, a preto sa niekedy volá aj **Hammingova metrika**.



Metrika na množine slov

Definícia

Reálna funkcia d definovaná na karteziánskom súčine $V \times V$ sa nazýva **metrikou na množine** *V, ak platí:*

1. *Pre každé $u, v \in V$ je $d(u, v) \geq 0$*
   a rovnosť nastáva práve vtedy, keď $u = v$.
2. *Pre každé $u, v \in V$ je $d(u, v) = d(v, u)$.*
3. *Ak $u, v, w \in V$, potom $d(u, w) \leq d(u, v) + d(v, w)$.*

Definícia

Hammingova vzdialenosť *$d(\mathbf{v}, \mathbf{w})$ dvoch slov $\mathbf{v} = v_1 v_2 \ldots v_n$,*
$\mathbf{w} = w_1 w_1 \ldots w_n$ je počet miest, na ktorých sa znaky slov $\mathbf{v}$, $\mathbf{w}$ líšia, t. j.

$$d(\mathbf{v}, \mathbf{w}) = \left|\{i \mid v_i \neq w_i, \quad i = 1, 2, \ldots, n\}\right|.$$

Ľahko sa dá ukázať, že Hammingova vzdialenosť má vlastnosti metriky, a preto sa niekedy volá aj **Hammingova metrika**.

Minimálna vzdialenosť kódu

Definícia

Minimálna vzdialenosť $\Delta(\mathcal{K})$ blokového kódu (K) *je minimum zo vzdialeností všetkých dvojíc rôznych slov kódu $\mathcal{K}$.*

$$\Delta(\mathcal{K}) = \min\{d(\mathbf{a}, \mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathcal{K},\ \mathbf{a} \neq \mathbf{b}\}. \tag{1}$$

Definícia

Hovoríme, že kód $\mathcal{K}$ **objavuje** *t-***násobné jednoduché chyby***, ak žiadne slovo $\mathbf{w}$ také, že $0 < d(\mathbf{w}, \mathbf{u}) \leq t$, kde $\mathbf{u}$ je kódové slovo, nie je kódovým slovom.*

Ak teda prijmeme nekódové slovo, hovoríme, že sme objavili chybu.

Všimnime si, že blokový kód $\mathcal{K}$ s minimálnou vzdialenosťou $\Delta(\mathcal{K}) = d$ objavuje $(d-1)$-násobné jednoduché chyby.

Minimálna vzdialenosť kódu

Definícia

Minimálna vzdialenosť $\Delta(\mathcal{K})$ **blokového kódu** (K) *je minimum zo vzdialeností všetkých dvojíc rôznych slov kódu* $\mathcal{K}$.

$$\Delta(\mathcal{K}) = \min\{d(\mathbf{a}, \mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathcal{K},\ \mathbf{a} \neq \mathbf{b}\}. \tag{1}$$

Definícia

Hovoríme, že kód $\mathcal{K}$ **objavuje** t**-násobné jednoduché chyby**, *ak žiadne slovo* $\mathbf{w}$ *také, že* $0 < d(\mathbf{w}, \mathbf{u}) \leq t$, *kde* $\mathbf{u}$ *je kódové slovo, nie je kódovým slovom.*

Ak teda prijmeme nekódové slovo, hovoríme, že sme objavili chybu.

Všimnime si, že blokový kód $\mathcal{K}$ s minimálnou vzdialenosťou $\Delta(\mathcal{K}) = d$ objavuje $(d-1)$-násobné jednoduché chyby.

Minimálna vzdialenosť kódu

Definícia

Minimálna vzdialenosť $\Delta(\mathcal{K})$ **blokového kódu** (K) *je minimum zo vzdialeností všetkých dvojíc rôznych slov kódu* $\mathcal{K}$.

$$\Delta(\mathcal{K}) = \min\{d(\mathbf{a}, \mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathcal{K},\ \mathbf{a} \neq \mathbf{b}\}. \tag{1}$$

Definícia

Hovoríme, že kód $\mathcal{K}$ **objavuje** t**-násobné jednoduché chyby**, *ak žiadne slovo* $\mathbf{w}$ *také, že* $0 < d(\mathbf{w}, \mathbf{u}) \leq t$, *kde* $\mathbf{u}$ *je kódové slovo, nie je kódovým slovom.*

Ak teda prijmeme nekódové slovo, hovoríme, že sme objavili chybu.

Všimnime si, že blokový kód $\mathcal{K}$ s minimálnou vzdialenosťou $\Delta(\mathcal{K}) = d$ objavuje $(d-1)$-násobné jednoduché chyby.

Kód dva z piatich

Príklad (Kód dva z piatich)

Dva prvky z piatich možno vybrať $\binom{5}{2} = 10$ *spôsobmi, čo možno využiť pre kódovanie dekadických cifier nasledovne:*

1	11000	6	00101
2	10100	7	00011
3	10010	8	00110
4	10001	9	01100
5	01001	0	01010

Kód dva z piatich objavuje jednu chybu – pri zmene ktorejkoľvek 0 na 1 vznikne nekódové slovo s troma znakmi 1, pri zmene 1 na 0 dostaneme nekódové slovo obsahujúce len jeden znak 1.

Kódové slová 11000 a 10100 majú však Hammingovu vzdialenosť rovnajúcu sa 2, z čoho vyplýva, že kód dva z piatich neobjavuje všetky 2-násobné jednoduché chyby.

Kód dva z piatich

Príklad (Kód dva z piatich)

Dva prvky z piatich možno vybrať $\binom{5}{2} = 10$ *spôsobmi, čo možno využiť pre kódovanie dekadických cifier nasledovne:*

1	*11000*	*6*	*00101*
2	*10100*	*7*	*00011*
3	*10010*	*8*	*00110*
4	*10001*	*9*	*01100*
5	*01001*	*0*	*01010*

Kód dva z piatich objavuje jednu chybu – pri zmene ktorejkoľvek 0 na 1 vznikne nekódové slovo s troma znakmi 1, pri zmene 1 na 0 dostaneme nekódové slovo obsahujúce len jeden znak 1.

Kódové slová 11000 a 10100 majú však Hammingovu vzdialenosť rovnajúcu sa 2, z čoho vyplýva, že kód dva z piatich neobjavuje všetky 2-násobné jednoduché chyby.

Kód dva z piatich

Príklad (Kód dva z piatich)

Dva prvky z piatich možno vybrať $\binom{5}{2} = 10$ *spôsobmi, čo možno využiť pre kódovanie dekadických cifier nasledovne:*

1	*11000*	*6*	*00101*
2	*10100*	*7*	*00011*
3	*10010*	*8*	*00110*
4	*10001*	*9*	*01100*
5	*01001*	*0*	*01010*

Kód dva z piatich objavuje jednu chybu – pri zmene ktorejkoľvek 0 na 1 vznikne nekódové slovo s troma znakmi 1, pri zmene 1 na 0 dostaneme nekódové slovo obsahujúce len jeden znak 1.

Kódové slová 11000 a 10100 majú však Hammingovu vzdialenosť rovnajúcu sa 2, z čoho vyplýva, že kód dva z piatich neobjavuje všetky 2-násobné jednoduché chyby.

Kód s kontrolou parity. Zdvojovací kód.

Príklad

Kód s kontrolou parity *je osembitový kód, kde prvých 7 bitov je ľubovoľný 7-miestny binárny blokový kód a kde je posledný binárny znak doplnený tak, aby počet jednotkových bitov bol párny.*
Kód s kontrolou parity objavuje jednu jednoduchú chybu, jeho minimálna vzdialenosť je 2.

Princíp kontroly paritou bol veľmi často používaný pri prenosoch a občas sa s ním stretneme aj v súčasnosti.

Príklad

Zdvojovací kód. *Ide o kód párnej dĺžky, v ktorom sa každý znak opakuje dvakrát. Zdvojovací binárny kód dĺžky 6 má osem kódových slov:*

000000 000011 001100 001111 110000 110011 111100 111111

Zdvojovací kód má minimálnu vzdialenosť 2, objavuje jednu jednoduchú chybu.

Kód s kontrolou parity. Zdvojovací kód.

Príklad

Kód s kontrolou parity *je osembitový kód, kde prvých 7 bitov je ľubovoľný 7-miestny binárny blokový kód a kde je posledný binárny znak doplnený tak, aby počet jednotkových bitov bol párny.*
Kód s kontrolou parity objavuje jednu jednoduchú chybu, jeho minimálna vzdialenosť je 2.

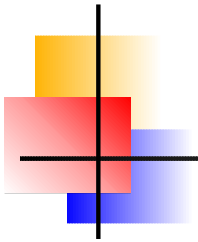
Princíp kontroly paritou bol veľmi často používaný pri prenosoch a občas sa s ním stretneme aj v súčasnosti.

Príklad

Zdvojovací kód. *Ide o kód párnej dĺžky, v ktorom sa každý znak opakuje dvakrát. Zdvojovací binárny kód dĺžky 6 má osem kódových slov:*

000000 000011 001100 001111 110000 110011 111100 111111

Zdvojovací kód má minimálnu vzdialenosť 2, objavuje jednu jednoduchú chybu.



Opakovací kód

Príklad

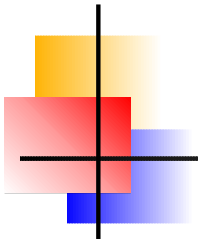
Opakovací kód. *Princípom opakovacieho kódu je niekoľkonásobné opakovanie toho istého znaku.*
Kódové slová sú len slová pozostávajúce z toho istého znaku – napr.

$$11111, \quad 22222, \quad \ldots, \quad 99999, \quad 00000.$$

Opakovací kód $\mathcal{K}$ dĺžky n má minimálnu vzdialenosť $\Delta\mathcal{K} = n$, a preto objavuje $(n-1)$-násobné jednoduché chyby.

Všimnime si, že za predpokladu, že nastali maximálne dve chyby, pri opakovacom kóde dĺžky 5 vieme zrekonštruovať pôvodné slovo.

Ak prijmeme 10191, za predpokladu vzniku maximálne dvoch chýb vieme, že bolo vyslané slovo 11111.



Opakovací kód

Príklad

Opakovací kód. *Princípom opakovacieho kódu je niekoľkonásobné opakovanie toho istého znaku.*
Kódové slová sú len slová pozostávajúce z toho istého znaku – napr.

$$11111, \quad 22222, \quad \ldots, \quad 99999, \quad 00000.$$

Opakovací kód $\mathcal{K}$ dĺžky n má minimálnu vzdialenosť $\Delta\mathcal{K} = n$, a preto objavuje $(n-1)$-násobné jednoduché chyby.

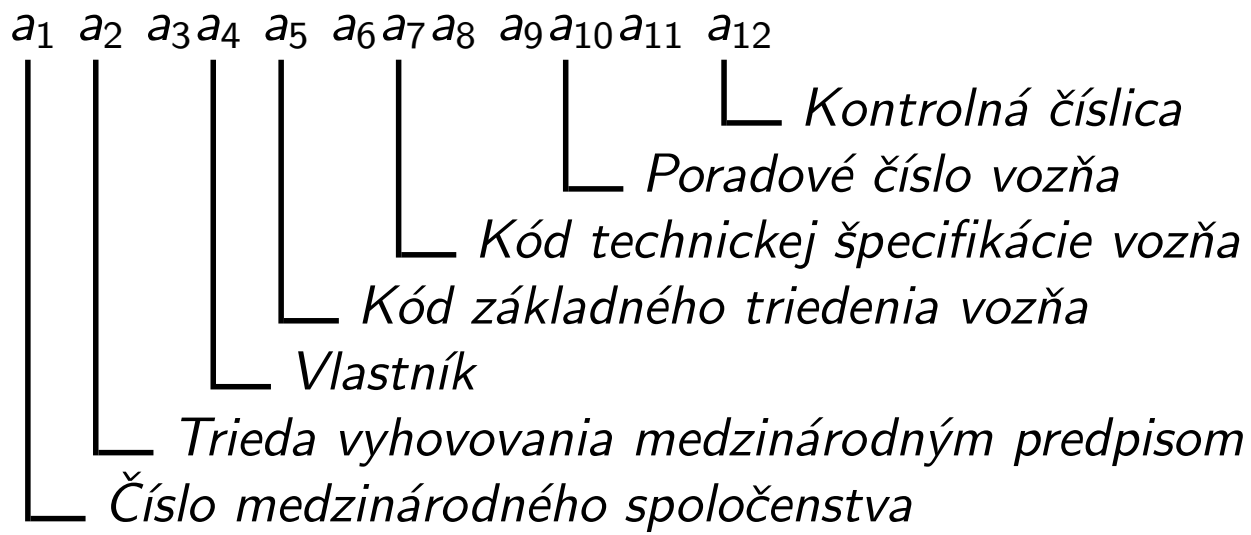
Všimnime si, že za predpokladu, že nastali maximálne dve chyby, pri opakovacom kóde dĺžky 5 vieme zrekonštruovať pôvodné slovo.

Ak prijmeme 10191, za predpokladu vzniku maximálne dvoch chýb vieme, že bolo vyslané slovo 11111.

Medzinárodné číslo vagónu

Príklad

Medzinárodné číslo vagónu *je 12-miestne dekadické číslo tvaru*



Majme číslo vagóna $a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10} a_{11} a_{12}$.

Kontrolná číslica a_{12} *sa určí tak, aby ciferný súčet čísel*

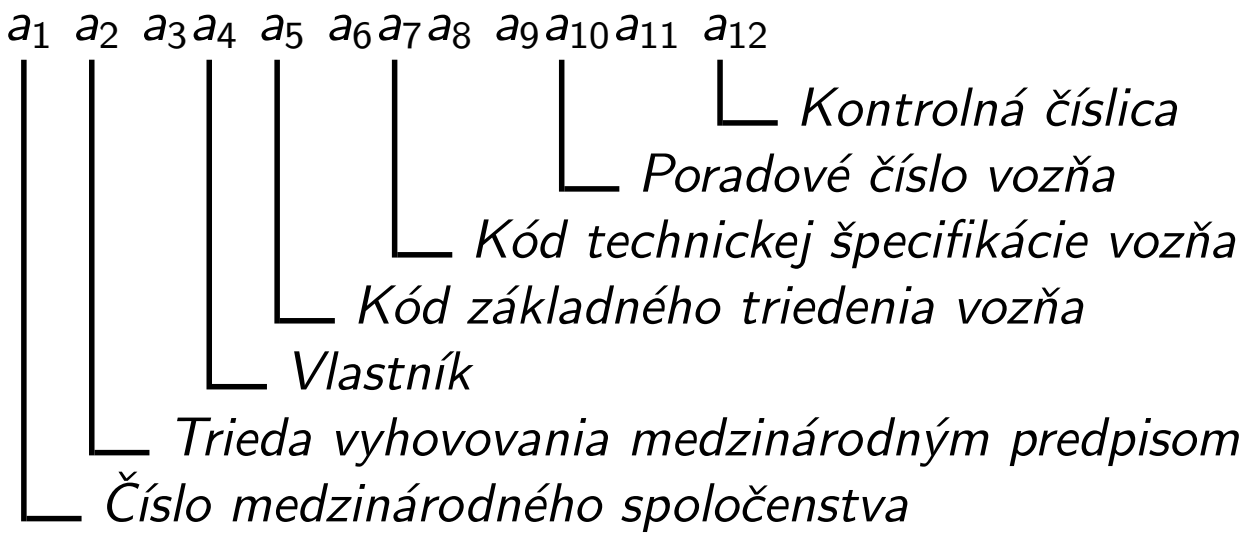
$$2a_1 \; a_2 \; 2a_3 \; a_4 \; 2a_5 \; a_6 \; 2a_7 \; a_8 \; 2a_9 \; a_{10} \; 2a_{11} \; a_{12}$$

bol deliteľný číslom 10.

Medzinárodné číslo vagónu

Príklad

Medzinárodné číslo vagónu *je 12-miestne dekadické číslo tvaru*



Majme číslo vagóna $a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10} a_{11} a_{12}$.

Kontrolná číslica a_{12} *sa určí tak, aby ciferný súčet čísel*

$$2a_1 \; a_2 \; 2a_3 \; a_4 \; 2a_5 \; a_6 \; 2a_7 \; a_8 \; 2a_9 \; a_{10} \; 2a_{11} \; a_{12}$$

bol deliteľný číslom 10.

Medzinárodné číslo vagónu

Označme $\delta(Y)$ ciferný súčet čísla $2Y$ pre $Y = 0, 1, \ldots, 9$.
Potom

$$\delta(Y) = \begin{cases} 2Y & \text{ak } Y \leq 4 \\ 2Y - 9 & \text{ak } Y > 4 \end{cases}$$

Nech na dvoch susedných miestach sú cifry C, D, nech C je na nepárnom mieste.
Hľadajme, pre ktoré hodnoty cifier C, D sa kontrolná číslica po ich susednej zámene nezmení.
Aby sa kontrolná číslica pri susednej zámene cifier nezmenila, musí dať súčet $\delta(C) + D$ ten istý zvyšok pri delení desiatimi ako $\delta(D) + C$ a teda ich rozdiel musí byť deliteľný desiatimi.

$$\delta(C)+D-\delta(D)-C = \begin{cases} 2C + D - 2D - C = C - D & \text{ak } C \leq 4 \text{ a } D \leq 4 \\ 2C - 9 + D - 2D - C = C - D - 9 & \text{ak } C \geq 5 \text{ a } D \leq 4 \\ 2C + D - 2D + 9 - C = C - D + 9 & \text{ak } C \leq 4 \text{ a } D \geq 5 \\ 2C + 9 + D - 2D - 9 - C = C - D & \text{ak } C \geq 5 \text{ a } D \geq 5 \end{cases}$$

Medzinárodné číslo vagónu

Označme $\delta(Y)$ ciferný súčet čísla $2Y$ pre $Y = 0, 1, \ldots, 9$.
Potom

$$\delta(Y) = \begin{cases} 2Y & \text{ak } Y \leq 4 \\ 2Y - 9 & \text{ak } Y > 4 \end{cases}$$

Nech na dvoch susedných miestach sú cifry C, D, nech C je na nepárnom mieste.
Hľadajme, pre ktoré hodnoty cifier C, D sa kontrolná číslica po ich susednej zámene nezmení.
Aby sa kontrolná číslica pri susednej zámene cifier nezmenila, musí dať súčet $\delta(C) + D$ ten istý zvyšok pri delení desiatimi ako $\delta(D) + C$ a teda ich rozdiel musí byť deliteľný desiatimi.

$$\delta(C)+D-\delta(D)-C = \begin{cases} 2C + D - 2D - C = C - D & \text{ak } C \leq 4 \text{ a } D \leq 4 \\ 2C - 9 + D - 2D - C = C - D - 9 & \text{ak } C \geq 5 \text{ a } D \leq 4 \\ 2C + D - 2D + 9 - C = C - D + 9 & \text{ak } C \leq 4 \text{ a } D \geq 5 \\ 2C + 9 + D - 2D - 9 - C = C - D & \text{ak } C \geq 5 \text{ a } D \geq 5 \end{cases}$$

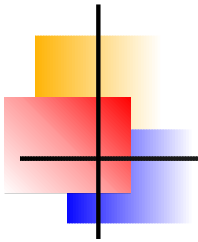
Medzinárodné číslo vagónu

Označme $\delta(Y)$ ciferný súčet čísla $2Y$ pre $Y = 0, 1, \ldots, 9$.
Potom

$$\delta(Y) = \begin{cases} 2Y & \text{ak } Y \leq 4 \\ 2Y - 9 & \text{ak } Y > 4 \end{cases}$$

Nech na dvoch susedných miestach sú cifry C, D, nech C je na nepárnom mieste.
Hľadajme, pre ktoré hodnoty cifier C, D sa kontrolná číslica po ich susednej zámene nezmení.
Aby sa kontrolná číslica pri susednej zámene cifier nezmenila, musí dať súčet $\delta(C) + D$ ten istý zvyšok pri delení desiatimi ako $\delta(D) + C$ a teda ich rozdiel musí byť deliteľný desiatimi.

$$\delta(C)+D-\delta(D)-C = \begin{cases} 2C + D - 2D - C = C - D & \text{ak } C \leq 4 \text{ a } D \leq 4 \\ 2C - 9 + D - 2D - C = C - D - 9 & \text{ak } C \geq 5 \text{ a } D \leq 4 \\ 2C + D - 2D + 9 - C = C - D + 9 & \text{ak } C \leq 4 \text{ a } D \geq 5 \\ 2C + 9 + D - 2D - 9 - C = C - D & \text{ak } C \geq 5 \text{ a } D \geq 5 \end{cases}$$



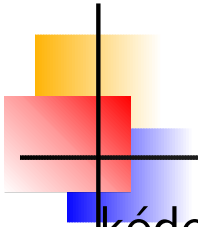
Medzinárodné číslo vagónu

Rovnica

$$\delta(C) + D - \delta(D) - C \equiv 0 \mod 10$$

má len dve riešenia, a to $C = 0$, $D = 9$ a $C = 9$, $D = 0$.

Kód medzinárodného čísla vozňa objavuje preklepy a susedné zámeny okrem dvojice (9,0) a (0,9).



Kontrola modulo 10

kódové slová tvorené znakmi a_1 až a_n sú práve tie slová, ktoré vyhovujú tzv. kontrolnej rovnici

$$\sum_{i=1}^{n} w_i.a_i \equiv c \mod 10 . \tag{2}$$

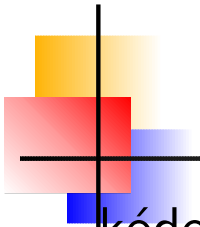
Ak sa v slove $a_1 a_2 \ldots a_n$ zmení a_j na a'_j, bude sa ľavá strana kontrolnej rovnice 2 pre takto zmenené slovo rovnať

$$\sum_{i=1}^{n} w_i.a_i + w_j.a'_j - w_j.a_j \equiv c + w_j.(a'_j - a_j) \mod 10 .$$

Pravá strana rovnice (2) sa nezmení a príslušný kód neobjaví jednoduchú chybu, ak

$$w_j.(a'_j - a_j) \equiv 0 \mod 10 .$$

Posledná rovnica má jediné riešenie $a'_j = a_j$ práve vtedy, keď w_j nie je súdeliteľné s číslom 10. Na miestach w_i môžu byť len čísla 1, 3, 7 a 9.



Kontrola modulo 10

kódové slová tvorené znakmi a_1 až a_n sú práve tie slová, ktoré vyhovujú tzv. kontrolnej rovnici

$$\sum_{i=1}^{n} w_i.a_i \equiv c \mod 10 . \tag{2}$$

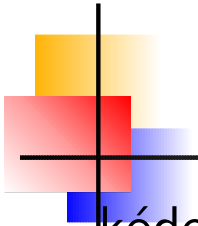
Ak sa v slove $a_1 a_2 \ldots a_n$ zmení a_j na a'_j, bude sa ľavá strana kontrolnej rovnice 2 pre takto zmenené slovo rovnať

$$\sum_{i=1}^{n} w_i.a_i + w_j.a'_j - w_j.a_j \equiv c + w_j.(a'_j - a_j) \mod 10 .$$

Pravá strana rovnice (2) sa nezmení a príslušný kód neobjaví jednoduchú chybu, ak

$$w_j.(a'_j - a_j) \equiv 0 \mod 10 .$$

Posledná rovnica má jediné riešenie $a'_j = a_j$ práve vtedy, keď w_j nie je súdeliteľné s číslom 10. Na miestach w_i môžu byť len čísla 1, 3, 7 a 9.



Kontrola modulo 10

kódové slová tvorené znakmi a_1 až a_n sú práve tie slová, ktoré vyhovujú tzv. kontrolnej rovnici

$$\sum_{i=1}^{n} w_i.a_i \equiv c \mod 10 . \tag{2}$$

Ak sa v slove $a_1 a_2 \ldots a_n$ zmení a_j na a'_j, bude sa ľavá strana kontrolnej rovnice 2 pre takto zmenené slovo rovnať

$$\sum_{i=1}^{n} w_i.a_i + w_j.a'_j - w_j.a_j \equiv c + w_j.(a'_j - a_j) \mod 10 .$$

Pravá strana rovnice (2) sa nezmení a príslušný kód neobjaví jednoduchú chybu, ak

$$w_j.(a'_j - a_j) \equiv 0 \mod 10 .$$

Posledná rovnica má jediné riešenie $a'_j = a_j$ práve vtedy, keď w_j nie je súdeliteľné s číslom 10. Na miestach w_i môžu byť len čísla 1, 3, 7 a 9.

Kontrola modulo 10

Kód nezistí susednú zámenu znakov x, y na miestach i, $i+1$ práve vtedy, keď

$$w_i.y + w_{i+1}.x - w_i.x - w_{i+1}.y \equiv 0 \mod 10$$
$$w_i.(y-x) - w_{i+1}.(y-x) \equiv 0 \mod 10$$
$$(w_i - w_{i+1})(y-x) \equiv 0 \mod 10$$

K tomu, aby posledná rovnica nemala okrem riešení $x = y$ žiadne ďalšie je nutné a stačí, aby $(w_i - w_{i+1})$ bolo nesúdeliteľné s 10. Ak má však kód s kontrolnou rovnicou (2) rozoznávať jednoduché chyby, musí byť $w_i \in \{1, 3, 7, 9\}$ a preto je $(w_i - w_{i+1})$ vždy párne.

Veta

Nech K je desiatkový blokový kód dĺžky n s kontrolnou rovnicou (2). Kód K objavuje jednoduché chyby práve vtedy, keď sú všetky w_i nesúdeliteľné s 10, t. j. $w_i \in \{1, 3, 7, 9\}$.
Žiaden desiatkový blokový kód dĺžky n s kontrolnou rovnicou (2) neobjavuje jednoduché chyby a súčasne aj susedné zámeny.

Kontrola modulo 10

Kód nezistí susednú zámenu znakov x, y na miestach i, $i+1$ práve vtedy, keď

$$\begin{aligned} w_i.y + w_{i+1}.x - w_i.x - w_{i+1}.y &\equiv 0 \mod 10 \\ w_i.(y-x) - w_{i+1}.(y-x) &\equiv 0 \mod 10 \\ (w_i - w_{i+1})(y-x) &\equiv 0 \mod 10 \end{aligned}$$

K tomu, aby posledná rovnica nemala okrem riešení $x = y$ žiadne ďalšie je nutné a stačí, aby $(w_i - w_{i+1})$ bolo nesúdeliteľné s 10. Ak má však kód s kontrolnou rovnicou (2) rozoznávať jednoduché chyby, musí byť $w_i \in \{1, 3, 7, 9\}$ a preto je $(w_i - w_{i+1})$ vždy párne.

Veta

Nech K je desiatkový blokový kód dĺžky n s kontrolnou rovnicou (2). Kód K objavuje jednoduché chyby práve vtedy, keď sú všetky w_i nesúdeliteľné s 10, t. j. $w_i \in \{1, 3, 7, 9\}$.
Žiaden desiatkový blokový kód dĺžky n s kontrolnou rovnicou (2) neobjavuje jednoduché chyby a súčasne aj susedné zámeny.

Kontrola modulo 10

Kód nezistí susednú zámenu znakov x, y na miestach i, $i+1$ práve vtedy, keď

$$\begin{aligned} w_i.y + w_{i+1}.x - w_i.x - w_{i+1}.y &\equiv 0 \mod 10 \\ w_i.(y-x) - w_{i+1}.(y-x) &\equiv 0 \mod 10 \\ (w_i - w_{i+1})(y-x) &\equiv 0 \mod 10 \end{aligned}$$

K tomu, aby posledná rovnica nemala okrem riešení $x = y$ žiadne ďalšie je nutné a stačí, aby $(w_i - w_{i+1})$ bolo nesúdeliteľné s 10. Ak má však kód s kontrolnou rovnicou (2) rozoznávať jednoduché chyby, musí byť $w_i \in \{1, 3, 7, 9\}$ a preto je $(w_i - w_{i+1})$ vždy párne.

Veta

Nech K je desiatkový blokový kód dĺžky n s kontrolnou rovnicou (2). Kód K objavuje jednoduché chyby práve vtedy, keď sú všetky w_i nesúdeliteľné s 10, t. j. $w_i \in \{1, 3, 7, 9\}$.
Žiaden desiatkový blokový kód dĺžky n s kontrolnou rovnicou (2) neobjavuje jednoduché chyby a súčasne aj susedné zámeny.

Kód EAN – European Article Number

$$1.9+3.0+1.0+3.2+1.8+3.4+1.3+3.2+1.0+3.3+1.2+3.6+1.7 = 80 \equiv 0 \mod 10$$

Kód EAN – European Article Number

Príklad

European Article Number je 13-miestny dekadický kód, ktorým sa jedinečne označujú výrobky v rámci Európy.
Prvých dvanásť znakov a_1 až a_{12} kódu EAN je významových, znak a_{13} je kontrolný a vypočíta sa z rovnice

$$a_{13} \equiv -(1.a_1 + 3.a_2 + 1.a_3 + 3.a_4 + \cdots + 1.a_{11} + 3.a_{12}) \mod 10 .$$

Kód EAN odhaľuje jednoduché chyby. Pre dvojicu znakov x, y, na dvoch susedných miestach nepárnom a párnom kód neodhalí susednú zámenu, ak

$$(x + 3y) - (3x + y) \equiv 0 \mod 10$$
$$(2y - 2x) \equiv 0 \mod 10$$
$$2.(y - x) \equiv 0 \mod 10$$

Posledná rovnica má tieto riešenia (x, y) také, že $x \neq y$:

$$(0,5),\ (1,6),\ (2,7),\ (3,8),\ (4,9),$$
$$(5,0),\ (6,1),\ (7,2),\ (8,3),\ (9,4)$$

Kód EAN – European Article Number

Príklad

European Article Number je 13-miestny dekadický kód, ktorým sa jedinečne označujú výrobky v rámci Európy.
Prvých dvanásť znakov a_1 až a_{12} kódu EAN je významových, znak a_{13} je kontrolný a vypočíta sa z rovnice

$$a_{13} \equiv -(1.a_1 + 3.a_2 + 1.a_3 + 3.a_4 + \cdots + 1.a_{11} + 3.a_{12}) \mod 10 \ .$$

Kód EAN odhaľuje jednoduché chyby. Pre dvojicu znakov x, y, na dvoch susedných miestach nepárnom a párnom kód neodhalí susednú zámenu, ak

$$\begin{aligned} (x + 3y) - (3x + y) &\equiv 0 \mod 10 \\ (2y - 2x) &\equiv 0 \mod 10 \\ 2.(y - x) &\equiv 0 \mod 10 \end{aligned}$$

Posledná rovnica má tieto riešenia (x, y) také, že $x \neq y$:

$$(0,5),\ (1,6),\ (2,7),\ (3,8),\ (4,9),$$
$$(5,0),\ (6,1),\ (7,2),\ (8,3),\ (9,4)$$

Kód EAN – European Article Number

Príklad

European Article Number je 13-miestny dekadický kód, ktorým sa jedinečne označujú výrobky v rámci Európy.
Prvých dvanásť znakov a_1 až a_{12} kódu EAN je významových, znak a_{13} je kontrolný a vypočíta sa z rovnice

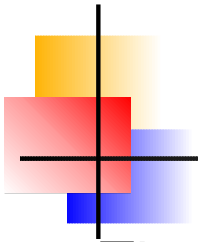
$$a_{13} \equiv -(1.a_1 + 3.a_2 + 1.a_3 + 3.a_4 + \cdots + 1.a_{11} + 3.a_{12}) \mod 10 \ .$$

Kód EAN odhaľuje jednoduché chyby. Pre dvojicu znakov x, y, na dvoch susedných miestach nepárnom a párnom kód neodhalí susednú zámenu, ak

$$\begin{aligned} (x + 3y) - (3x + y) &\equiv 0 \mod 10 \\ (2y - 2x) &\equiv 0 \mod 10 \\ 2.(y - x) &\equiv 0 \mod 10 \end{aligned}$$

Posledná rovnica má tieto riešenia (x, y) také, že $x \neq y$:

$$(0,5),\ (1,6),\ (2,7),\ (3,8),\ (4,9),$$
$$(5,0),\ (6,1),\ (7,2),\ (8,3),\ (9,4)$$



Kontrola modulo 11

Tieto kódy pracujú s kódovou abecedou $B \cup \{X\}$, kde znak X nahradzuje číslicu 10, $B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\}$, pričom kódové slová majú všetkých prvých $n - 1$ znakov z abecedy B a posledný – kontrolný znak a_n z abecedy $B \cup \{X\}$ je určený tak, aby platila nasledujúca kontrolná rovnica

$$\sum_{i=1}^{n} w_i.a_i \equiv c \mod 11 , \quad \text{kde } 0 < w_i \leq 10 \text{ pre } i = 1, 2, \ldots, n . \qquad (3)$$

Podobne ako v prípade kontroly modulo 10 ukážeme, že kód kontroly modulo 11 objavuje jednoduché chyby na mieste j práve vtedy, keď rovnica

$$w_j.(a'_j - a_j) \equiv 0 \mod 11$$

nemá okrem $a'_j = a_j$ žiadne iné riešenia, a to je práve vtedy, keď w_j je nesúdeliteľné s 11 na čo stačí, aby $w_j \neq 0$.

Kontrola modulo 11

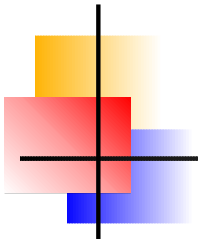
Tieto kódy pracujú s kódovou abecedou $B \cup \{X\}$, kde znak X nahradzuje číslicu 10, $B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\}$, pričom kódové slová majú všetkých prvých $n - 1$ znakov z abecedy B a posledný – kontrolný znak a_n z abecedy $B \cup \{X\}$ je určený tak, aby platila nasledujúca kontrolná rovnica

$$\sum_{i=1}^{n} w_i.a_i \equiv c \mod 11 , \quad \text{kde } 0 < w_i \leq 10 \text{ pre } i = 1, 2, \ldots, n . \qquad (3)$$

Podobne ako v prípade kontroly modulo 10 ukážeme, že kód kontroly modulo 11 objavuje jednoduché chyby na mieste j práve vtedy, keď rovnica

$$w_j.(a'_j - a_j) \equiv 0 \mod 11$$

nemá okrem $a'_j = a_j$ žiadne iné riešenia, a to je práve vtedy, keď w_j je nesúdeliteľné s 11 na čo stačí, aby $w_j \neq 0$.



Kontrola modulo 11

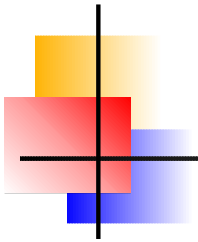
Na to, aby kód s kontrolou modulo 11 objavoval susedné zámeny na miestach i, $i+1$ stačí, aby rovnica

$$(w_i - w_{i+1}).(y - x) \equiv 0 \mod 11$$

okrem riešení, kde $x = y$ nemala žiadne iné riešenia. Na to však stačí, aby $w_i \neq w_{i+1}$.

Mnoho dobrých vlastností má tzv. **geometrický kód modulo 11**, kde čísla w_i v kontrolnej rovnici (3) sú určené ako

$$w_i = 2^i \mod 11 .$$



Kontrola modulo 11

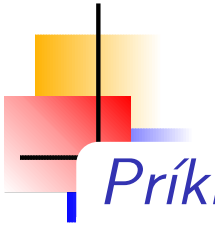
Na to, aby kód s kontrolou modulo 11 objavoval susedné zámeny na miestach i, $i+1$ stačí, aby rovnica

$$(w_i - w_{i+1}).(y - x) \equiv 0 \mod 11$$

okrem riešení, kde $x = y$ nemala žiadne iné riešenia. Na to však stačí, aby $w_i \neq w_{i+1}$.

Mnoho dobrých vlastností má tzv. **geometrický kód modulo 11**, kde čísla w_i v kontrolnej rovnici (3) sú určené ako

$$w_i = 2^i \mod 11 \ .$$



Kontrola modulo 11

Príklad

ISBN – *International Standard Book Number je 10 miestne číslo prideľované každej oficiálne vydanej knihe.*
Prvé štyri znaky $a_1 a_2 a_3 a_4$ určujú krajinu a vydavateľstvo, ďalších päť znakov $a_5 a_6 a_7 a_8 a_9$ predstavuje číslo knihy v rámci špecifikovaného vydavateľstva a posledný znak a_{10} je kontrolný znak určený rovnicou

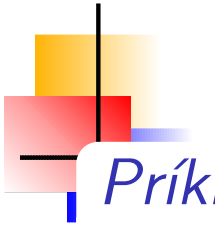
$$a_{10} \equiv \sum_{i=1}^{9} i.a_i \mod 11 \ .$$

Znaky a_1 až a_9 sú z abecedy $B = \{0, 1, \ldots, 9\}$, znak a_{10} je z abecedy $B \cup \{X\}$, kde znak X predstavuje hodnotu 10.

Posledná rovnica je totožná s rovnicou

$$\sum_{i=1}^{10} i.a_i \equiv 0 \mod 11 \ ,$$

pretože $-a_{10} \equiv -a_{10} + 11.a_{10} \equiv 10.a_{10} \mod 11$. Ak $a_{10} = 10$, píše sa na mieste a_{10} znak X.
ISBN kód objavuje všetky jednoduché chyby a všetky susedné zámeny.



Kontrola modulo 11

Príklad

ISBN – *International Standard Book Number je 10 miestne číslo prideľované každej oficiálne vydanej knihe.*
Prvé štyri znaky $a_1 a_2 a_3 a_4$ určujú krajinu a vydavateľstvo, ďalších päť znakov $a_5 a_6 a_7 a_8 a_9$ predstavuje číslo knihy v rámci špecifikovaného vydavateľstva a posledný znak a_{10} je kontrolný znak určený rovnicou

$$a_{10} \equiv \sum_{i=1}^{9} i.a_i \mod 11 \ .$$

Znaky a_1 až a_9 sú z abecedy $B = \{0, 1, \ldots, 9\}$, znak a_{10} je z abecedy $B \cup \{X\}$, kde znak X predstavuje hodnotu 10.

Posledná rovnica je totožná s rovnicou

$$\sum_{i=1}^{10} i.a_i \equiv 0 \mod 11 \ ,$$

pretože $-a_{10} \equiv -a_{10} + 11.a_{10} \equiv 10.a_{10} \mod 11$. Ak $a_{10} = 10$, píše sa na mieste a_{10} znak X.
ISBN kód objavuje všetky jednoduché chyby a všetky susedné zámeny.

Kontrola modulo 11

Príklad

ISBN – *International Standard Book Number je 10 miestne číslo prideľované každej oficiálne vydanej knihe.*
Prvé štyri znaky $a_1 a_2 a_3 a_4$ určujú krajinu a vydavateľstvo, ďalších päť znakov $a_5 a_6 a_7 a_8 a_9$ predstavuje číslo knihy v rámci špecifikovaného vydavateľstva a posledný znak a_{10} je kontrolný znak určený rovnicou

$$a_{10} \equiv \sum_{i=1}^{9} i.a_i \mod 11 \ .$$

Znaky a_1 až a_9 sú z abecedy $B = \{0, 1, \ldots, 9\}$, znak a_{10} je z abecedy $B \cup \{X\}$, kde znak X predstavuje hodnotu 10.

Posledná rovnica je totožná s rovnicou

$$\sum_{i=1}^{10} i.a_i \equiv 0 \mod 11 \ ,$$

pretože $-a_{10} \equiv -a_{10} + 11.a_{10} \equiv 10.a_{10} \mod 11$. Ak $a_{10} = 10$, píše sa na mieste a_{10} znak X.
ISBN kód objavuje všetky jednoduché chyby a všetky susedné zámeny.

Čísla bankových účtov slovenských bánk

Príklad

Čísla bankových účtov slovenských bánk. *Číslo bankového účtu je desaťmiestne dekadické číslo*

$$a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9.$$

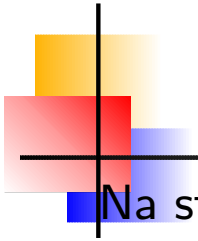
Význam jednotlivých pozícií Národná banka Slovenska nešpecifikuje, avšak pre všetky banky platí rovnaký kontrolný mechanizmus.
Platné číslo bankového účtu musí vyhovovať kontrolnej rovnici

$$0 = \left(\sum_{i=0}^{9} 2^i.a_i\right) \mod 11 =$$

$$= (1.a_0 + 2.a_1 + 4.a_2 + 8.a_3 + \cdots + 512.a_9) \mod 11 =$$

$$= (a_0 + 2a_1 + 4a_2 + 8a_3 + 5a_4 + 10a_5 + 9a_6 + 7a_7 + 3a_8 + 6a_9) \mod 11 .$$

Tu je použitý geometrický kód modulo 11.
Kód bankových účtov teda odhaľuje okrem jednoduchých chýb aj všetky susedné zámeny, ba navyše aj vzájomné zámeny znakov na rôznych pozíciách čísla účtu.



Rodné číslo

Na stránke www.minv.sk/vediet/rc.html je uvedená nasledujúca špecifikácia:
Rodné číslo je definované v zákone ako číselný identifikačný osobný údaj, vytvorený z dátumu narodenia osoby, jej pohlavia a rozlišovacej koncovky.
Rodné číslo má tvar RRMMDDKKKK, kde

- RR vyjadruje posledné dve číslice roku narodenia osoby.
- MM vyjadruje mesiac narodenia a pohlavie osoby (napr. pre muža narodeného v januári je to dvojčíslie 01 pre ženu 51, pre muža narodeného v decembri je to dvojčíslie 12 a pre ženu 62).
- DD vyjadruje deň narodenia osoby (napr. pre osoby narodené v 1. deň mesiaca je to dvojčíslie 01, pre osoby narodené 15. deň je to dvojčíslie 15).
- KKKK je rozlišujúca koncovka pre osoby narodené v ten istý deň. Pre osoby narodené pred 1.1.1954 je koncovka trojmiestne číslo, pre osoby narodené po 31.12.1954 je koncovka štvormiestne číslo.

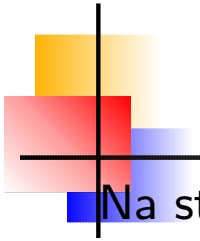
Napríklad muž narodený 31.12.1925 môže mať rodné číslo 251231 123,
žena narodená v ten istý deň 256231 123,
muž narodený 1.1.1954 môže mať rodné číslo 540101 4311, žena 545101 1324.
Desaťmiestne rodné číslo musí byť deliteľné číslom 11, pre deväťmiestne rodné číslo uvedená podmienka neplatí.

Rodné číslo

Na stránke www.minv.sk/vediet/rc.html je uvedená nasledujúca špecifikácia:
Rodné číslo je definované v zákone ako číselný identifikačný osobný údaj, vytvorený z dátumu narodenia osoby, jej pohlavia a rozlišovacej koncovky.
Rodné číslo má tvar RRMMDDKKKK, kde

- RR vyjadruje posledné dve číslice roku narodenia osoby.
- MM vyjadruje mesiac narodenia a pohlavie osoby (napr. pre muža narodeného v januári je to dvojčíslie 01 pre ženu 51, pre muža narodeného v decembri je to dvojčíslie 12 a pre ženu 62).
- DD vyjadruje deň narodenia osoby (napr. pre osoby narodené v 1. deň mesiaca je to dvojčíslie 01, pre osoby narodené 15. deň je to dvojčíslie 15).
- KKKK je rozlišujúca koncovka pre osoby narodené v ten istý deň. Pre osoby narodené pred 1.1.1954 je koncovka trojmiestne číslo, pre osoby narodené po 31.12.1954 je koncovka štvormiestne číslo.

Napríklad muž narodený 31.12.1925 môže mať rodné číslo 251231 123,
žena narodená v ten istý deň 256231 123,
muž narodený 1.1.1954 môže mať rodné číslo 540101 4311, žena 545101 1324.
Desaťmiestne rodné číslo musí byť deliteľné číslom 11, pre deväťmiestne rodné číslo uvedená podmienka neplatí.



Rodné číslo

Na stránke www.minv.sk/vediet/rc.html je uvedená nasledujúca špecifikácia:
Rodné číslo je definované v zákone ako číselný identifikačný osobný údaj, vytvorený z dátumu narodenia osoby, jej pohlavia a rozlišovacej koncovky.
Rodné číslo má tvar RRMMDDKKKK, kde

- RR vyjadruje posledné dve číslice roku narodenia osoby.
- MM vyjadruje mesiac narodenia a pohlavie osoby (napr. pre muža narodeného v januári je to dvojčíslie 01 pre ženu 51, pre muža narodeného v decembri je to dvojčíslie 12 a pre ženu 62).
- DD vyjadruje deň narodenia osoby (napr. pre osoby narodené v 1. deň mesiaca je to dvojčíslie 01, pre osoby narodené 15. deň je to dvojčíslie 15).
- KKKK je rozlišujúca koncovka pre osoby narodené v ten istý deň. Pre osoby narodené pred 1.1.1954 je koncovka trojmiestne číslo, pre osoby narodené po 31.12.1954 je koncovka štvormiestne číslo.

Napríklad muž narodený 31.12.1925 môže mať rodné číslo 251231 123,
žena narodená v ten istý deň 256231 123,
muž narodený 1.1.1954 môže mať rodné číslo 540101 4311, žena 545101 1324.
Desaťmiestne rodné číslo musí byť deliteľné číslom 11, pre deväťmiestne rodné číslo uvedená podmienka neplatí.

Rodné číslo

Na stránke www.minv.sk/vediet/rc.html je uvedená nasledujúca špecifikácia:
Rodné číslo je definované v zákone ako číselný identifikačný osobný údaj, vytvorený z dátumu narodenia osoby, jej pohlavia a rozlišovacej koncovky. Rodné číslo má tvar RRMMDDKKKK, kde

- RR vyjadruje posledné dve číslice roku narodenia osoby.
- MM vyjadruje mesiac narodenia a pohlavie osoby (napr. pre muža narodeného v januári je to dvojčíslie 01 pre ženu 51, pre muža narodeného v decembri je to dvojčíslie 12 a pre ženu 62).
- DD vyjadruje deň narodenia osoby (napr. pre osoby narodené v 1. deň mesiaca je to dvojčíslie 01, pre osoby narodené 15. deň je to dvojčíslie 15).
- KKKK je rozlišujúca koncovka pre osoby narodené v ten istý deň. Pre osoby narodené pred 1.1.1954 je koncovka trojmiestne číslo, pre osoby narodené po 31.12.1954 je koncovka štvormiestne číslo.

Napríklad muž narodený 31.12.1925 môže mať rodné číslo 251231 123,
žena narodená v ten istý deň 256231 123,
muž narodený 1.1.1954 môže mať rodné číslo 540101 4311, žena 545101 1324.
Desaťmiestne rodné číslo musí byť deliteľné číslom 11, pre deväťmiestne rodné číslo uvedená podmienka neplatí.

Rodné číslo

Na stránke www.minv.sk/vediet/rc.html je uvedená nasledujúca špecifikácia:
Rodné číslo je definované v zákone ako číselný identifikačný osobný údaj, vytvorený z dátumu narodenia osoby, jej pohlavia a rozlišovacej koncovky. Rodné číslo má tvar RRMMDDKKKK, kde

- RR vyjadruje posledné dve číslice roku narodenia osoby.
- MM vyjadruje mesiac narodenia a pohlavie osoby (napr. pre muža narodeného v januári je to dvojčíslie 01 pre ženu 51, pre muža narodeného v decembri je to dvojčíslie 12 a pre ženu 62).
- DD vyjadruje deň narodenia osoby (napr. pre osoby narodené v 1. deň mesiaca je to dvojčíslie 01, pre osoby narodené 15. deň je to dvojčíslie 15).
- KKKK je rozlišujúca koncovka pre osoby narodené v ten istý deň. Pre osoby narodené pred 1.1.1954 je koncovka trojmiestne číslo, pre osoby narodené po 31.12.1954 je koncovka štvormiestne číslo.

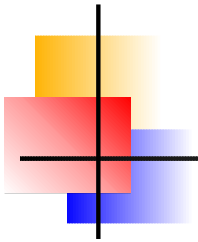
Napríklad muž narodený 31.12.1925 môže mať rodné číslo 251231 123,
žena narodená v ten istý deň 256231 123,
muž narodený 1.1.1954 môže mať rodné číslo 540101 4311, žena 545101 1324.
Desaťmiestne rodné číslo musí byť deliteľné číslom 11, pre deväťmiestne rodné číslo uvedená podmienka neplatí.

Rodné číslo

Na stránke www.minv.sk/vediet/rc.html je uvedená nasledujúca špecifikácia:
Rodné číslo je definované v zákone ako číselný identifikačný osobný údaj, vytvorený z dátumu narodenia osoby, jej pohlavia a rozlišovacej koncovky. Rodné číslo má tvar RRMMDDKKKK, kde

- RR vyjadruje posledné dve číslice roku narodenia osoby.
- MM vyjadruje mesiac narodenia a pohlavie osoby (napr. pre muža narodeného v januári je to dvojčíslie 01 pre ženu 51, pre muža narodeného v decembri je to dvojčíslie 12 a pre ženu 62).
- DD vyjadruje deň narodenia osoby (napr. pre osoby narodené v 1. deň mesiaca je to dvojčíslie 01, pre osoby narodené 15. deň je to dvojčíslie 15).
- KKKK je rozlišujúca koncovka pre osoby narodené v ten istý deň. Pre osoby narodené pred 1.1.1954 je koncovka trojmiestne číslo, pre osoby narodené po 31.12.1954 je koncovka štvormiestne číslo.

Napríklad muž narodený 31.12.1925 môže mať rodné číslo 251231 123,
žena narodená v ten istý deň 256231 123,
muž narodený 1.1.1954 môže mať rodné číslo 540101 4311, žena 545101 1324.
Desaťmiestne rodné číslo musí byť deliteľné číslom 11, pre deväťmiestne rodné číslo uvedená podmienka neplatí.



Rodné číslo

Majme desaťmiestne rodné číslo $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9$.
Z podmienky deliteľnosti rodného čísla číslom 11 vyplýva nasledujúca kontrolná rovnica:

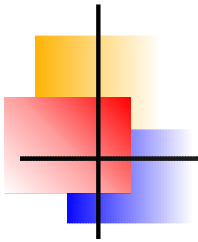
$$\sum_{i=0}^{9} 10^i . a_i \equiv 0 \mod 11 \ .$$

Ak je i párne číslo, t. j. $i = 2k$, potom $10^i = 10^{2k} = 100^k = (99+1)^k$.
Podľa binomickej vety môžeme písať

$$(99+1)^k = \binom{k}{k} 99^k + \binom{k}{k-1} 99^{k-1} + \cdots + \binom{k}{1} 99^1 + 1 \ .$$

Keďže číslo 99 je deliteľné jedenástimi, z posledného vyjadrenia máme

$$10^i \equiv 1 \mod 11 \quad \text{pre } i \text{ párne.}$$



Rodné číslo

Majme desaťmiestne rodné číslo $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9$.
Z podmienky deliteľnosti rodného čísla číslom 11 vyplýva nasledujúca kontrolná rovnica:

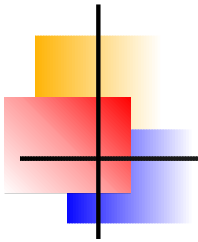
$$\sum_{i=0}^{9} 10^i . a_i \equiv 0 \mod 11 \ .$$

Ak je i párne číslo, t. j. $i = 2k$, potom $10^i = 10^{2k} = 100^k = (99+1)^k$.
Podľa binomickej vety môžeme písať

$$(99+1)^k = \binom{k}{k} 99^k + \binom{k}{k-1} 99^{k-1} + \cdots + \binom{k}{1} 99^1 + 1 \ .$$

Keďže číslo 99 je deliteľné jedenástimi, z posledného vyjadrenia máme

$$10^i \equiv 1 \mod 11 \quad \text{pre } i \text{ párne.}$$



Rodné číslo

Majme desaťmiestne rodné číslo $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9$.
Z podmienky deliteľnosti rodného čísla číslom 11 vyplýva nasledujúca kontrolná rovnica:

$$\sum_{i=0}^{9} 10^i . a_i \equiv 0 \mod 11 \ .$$

Ak je i párne číslo, t. j. $i = 2k$, potom $10^i = 10^{2k} = 100^k = (99+1)^k$.
Podľa binomickej vety môžeme písať

$$(99+1)^k = \binom{k}{k} 99^k + \binom{k}{k-1} 99^{k-1} + \cdots + \binom{k}{1} 99^1 + 1 \ .$$

Keďže číslo 99 je deliteľné jedenástimi, z posledného vyjadrenia máme

$$10^i \equiv 1 \mod 11 \quad \text{pre } i \text{ párne.}$$

Rodné číslo

Ak je i nepárne, t. j. $i = 2k+1$, potom $10^i = 10^{2k+1} = 10.100^k = 10.(99+1)^k$.

$$10.(99+1)^k = 10.\left[\binom{k}{k}99^k + \binom{k}{k-1}99^{k-1} + \cdots + \binom{k}{1}99^1 + 1\right] =$$

$$= 10.\binom{k}{k}99^k + 10.\binom{k}{k-1}99^{k-1} + \cdots + 10.\binom{k}{1}99^1 + 10\ .$$

Z posledného vzťahu máme

$$10^i \equiv 10 \mod 11 \quad \text{pre } i \text{ nepárne.}$$

Kontrolná rovnica desaťmiestneho rodného čísla má teda tvar

$$a_0 + 10a_1 + a_2 + 10a_3 + a_4 + 10a_5 + a_6 + 10a_7 + a_8 + 10a_9 \equiv 0 \mod 11\ . \quad (4)$$

Kód desaťmiestnych rodných čísel objavuje okrem jednoduchých chýb aj susedné zámeny.

Poznámka

Ľahko sa overí, že ekvivalentná rovnica s kontrolnou rovnicou (4) *je rovnica*

$$a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + a_6 - a_7 + a_8 - a_9 \equiv 0 \mod 11.$$

Rodné číslo

Ak je i nepárne, t. j. $i = 2k+1$, potom $10^i = 10^{2k+1} = 10.100^k = 10.(99+1)^k$.

$$10.(99+1)^k = 10.\left[\binom{k}{k}99^k + \binom{k}{k-1}99^{k-1} + \cdots + \binom{k}{1}99^1 + 1\right] =$$

$$= 10.\binom{k}{k}99^k + 10.\binom{k}{k-1}99^{k-1} + \cdots + 10.\binom{k}{1}99^1 + 10\ .$$

Z posledného vzťahu máme

$$10^i \equiv 10 \mod 11 \quad \text{pre } i \text{ nepárne.}$$

Kontrolná rovnica desaťmiestneho rodného čísla má teda tvar

$$a_0 + 10a_1 + a_2 + 10a_3 + a_4 + 10a_5 + a_6 + 10a_7 + a_8 + 10a_9 \equiv 0 \mod 11\ . \quad (4)$$

Kód desaťmiestnych rodných čísel objavuje okrem jednoduchých chýb aj susedné zámeny.

Poznámka

Ľahko sa overí, že ekvivalentná rovnica s kontrolnou rovnicou (4) *je rovnica*

$$a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + a_6 - a_7 + a_8 - a_9 \equiv 0 \mod 11.$$

Rodné číslo

Ak je i nepárne, t. j. $i = 2k+1$, potom $10^i = 10^{2k+1} = 10.100^k = 10.(99+1)^k$.

$$10.(99+1)^k = 10.\left[\binom{k}{k}99^k + \binom{k}{k-1}99^{k-1} + \cdots + \binom{k}{1}99^1 + 1\right] =$$

$$= 10.\binom{k}{k}99^k + 10.\binom{k}{k-1}99^{k-1} + \cdots + 10.\binom{k}{1}99^1 + 10\ .$$

Z posledného vzťahu máme

$$10^i \equiv 10 \mod 11 \quad \text{pre } i \text{ nepárne.}$$

Kontrolná rovnica desaťmiestneho rodného čísla má teda tvar

$$a_0 + 10a_1 + a_2 + 10a_3 + a_4 + 10a_5 + a_6 + 10a_7 + a_8 + 10a_9 \equiv 0 \mod 11\ . \quad (4)$$

Kód desaťmiestnych rodných čísel objavuje okrem jednoduchých chýb aj susedné zámeny.

Poznámka

Ľahko sa overí, že ekvivalentná rovnica s kontrolnou rovnicou (4) je rovnica

$$a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + a_6 - a_7 + a_8 - a_9 \equiv 0 \mod 11.$$

Rodné číslo

Ak je i nepárne, t. j. $i = 2k+1$, potom $10^i = 10^{2k+1} = 10.100^k = 10.(99+1)^k$.

$$10.(99+1)^k = 10.\left[\binom{k}{k}99^k + \binom{k}{k-1}99^{k-1} + \cdots + \binom{k}{1}99^1 + 1\right] =$$

$$= 10.\binom{k}{k}99^k + 10.\binom{k}{k-1}99^{k-1} + \cdots + 10.\binom{k}{1}99^1 + 10\ .$$

Z posledného vzťahu máme

$$10^i \equiv 10 \mod 11 \quad \text{pre } i \text{ nepárne.}$$

Kontrolná rovnica desaťmiestneho rodného čísla má teda tvar

$$a_0 + 10a_1 + a_2 + 10a_3 + a_4 + 10a_5 + a_6 + 10a_7 + a_8 + 10a_9 \equiv 0 \mod 11\ . \quad (4)$$

Kód desaťmiestnych rodných čísel objavuje okrem jednoduchých chýb aj susedné zámeny.

Poznámka

Ľahko sa overí, že ekvivalentná rovnica s kontrolnou rovnicou (4) *je rovnica*

$$a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + a_6 - a_7 + a_8 - a_9 \equiv 0 \mod 11.$$

Permutácie v kontrolnej rovnici mod 10

Kód s kontrolnou rovnicou $\sum_{i=1}^{n} w_i.a_i \equiv c \mod 10$ nedokáže odhaliť všetky preklepy a susedné zámeny.

Vzniká teda myšlienka nahradiť členy $w_i.a_i$ kontrolnej rovnice permutáciami $\delta_i(a_i)$. Kontrolná rovnica bude mať tvar:

$$\sum_{i=1}^{n} \delta_i(a_i) \equiv c \mod 10 .$$

Príklad

Medzinárodné číslo vozňa *je vlastne kód s permutáciami*

$$\delta_1 = \delta_3 = \cdots = \delta_{11} := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 & 9 \end{pmatrix}$$

$$\delta_2 = \delta_4 = \cdots = \delta_{12} := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$$

a s kontrolnou rovnicou $\sum_{i=1}^{12} \delta_i(a_i) \equiv 0 \mod 10 .$

Permutácie v kontrolnej rovnici mod 10

Kód s kontrolnou rovnicou $\sum_{i=1}^{n} w_i.a_i \equiv c \mod 10$ nedokáže odhaliť všetky preklepy a susedné zámeny.

Vzniká teda myšlienka nahradiť členy $w_i.a_i$ kontrolnej rovnice permutáciami $\delta_i(a_i)$. Kontrolná rovnica bude mať tvar:

$$\sum_{i=1}^{n} \delta_i(a_i) \equiv c \mod 10 .$$

Príklad

Medzinárodné číslo vozňa *je vlastne kód s permutáciami*

$$\delta_1 = \delta_3 = \cdots = \delta_{11} := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 & 9 \end{pmatrix}$$

$$\delta_2 = \delta_4 = \cdots = \delta_{12} := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$$

a s kontrolnou rovnicou $\sum_{i=1}^{12} \delta_i(a_i) \equiv 0 \mod 10 .$

Kód nemeckých poštových poukážok

Príklad

Kód nemeckých poštových poukážok *je desaťmiestny dekadický kód* $a_1 a_2 \ldots a_{10}$ *s kontrolným znakom* a_{10} *s kontrolnou rovnicou*

$$\sum_{i=1}^{10} \delta_i(a_i) \equiv 0 \mod 10 \ ,$$

kde

$$\delta_1 = \delta_4 = \delta_7 = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 1\,2\,3\,4\,5\,6\,7\,8\,9\,0 \end{pmatrix}$$

$$\delta_2 = \delta_5 = \delta_8 = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 2\,4\,6\,8\,0\,1\,3\,5\,7\,9 \end{pmatrix}$$

$$\delta_3 = \delta_6 = \delta_9 = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 3\,6\,9\,1\,4\,7\,0\,2\,5\,8 \end{pmatrix}$$

$$\delta_{10} = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 0\,9\,8\,7\,6\,5\,4\,3\,2\,1 \end{pmatrix}$$

Kódy s kontrolným znakom nad grupou – 1

Ani jeden z uvedených kódov kontroly modulo 10 neobjavuje všetky susedné zámeny.
Preto ďalším zovšeobecnením je nahradenie grupy zvyškových tried s grupovou operáciou $a \oplus b = (a + b) \mod 10$ nejakou inou grupou $\mathbb{G} = (A, *)$ a kontrolnú rovnicu formulovať ako

$$\prod_{i=1}^{n} \delta_i(a_i) = c \ . \tag{5}$$

Multiplikatívny tvar grupovej operácie $*$ naznačuje, že grupa $\mathbb{G}$ nemusí byť komutatívna.

Definícia

Nech A je abeceda, nech $\mathbb{G} = (A, *)$ je grupa. Nech $\delta_1, \delta_2, \ldots, \delta_n$, sú permutácie na A. Potom kontrolnou rovnicou (5) definovaný kód nazveme **kód s kontrolným znakom nad grupou** $\mathbb{G}$.

Kódy s kontrolným znakom nad grupou – 1

Ani jeden z uvedených kódov kontroly modulo 10 neobjavuje všetky susedné zámeny.
Preto ďalším zovšeobecnením je nahradenie grupy zvyškových tried s grupovou operáciou $a \oplus b = (a + b) \mod 10$ nejakou inou grupou $\mathbb{G} = (A, *)$ a kontrolnú rovnicu formulovať ako

$$\prod_{i=1}^{n} \delta_i(a_i) = c \ . \tag{5}$$

Multiplikatívny tvar grupovej operácie $*$ naznačuje, že grupa $\mathbb{G}$ nemusí byť komutatívna.

Definícia

Nech A je abeceda, nech $\mathbb{G} = (A, *)$ je grupa. Nech $\delta_1, \delta_2, \ldots, \delta_n$, sú permutácie na A. Potom kontrolnou rovnicou (5) *definovaný kód nazveme* **kód s kontrolným znakom nad grupou** $\mathbb{G}$.

Kódy s kontrolným znakom nad grupou – 2

Veta (1.)

Aby kód $\mathcal{K}$ s kontrolným znakom nad grupou $\mathbb{G} = (A, *)$ rozpoznal zámenu ľubovoľných susedných znakov na miestach i, $i+1$ je nevyhnutné a stačí, aby

$$x * \delta_{i+1} \circ \delta_i^{-1}(y) \neq y * \delta_{i+1} \circ \delta_i^{-1}(x) \tag{6}$$

pre všetky $x \in A$, $y \in A$, $x \neq y$.

Pre Abelovu grupu $\mathbb{G} = (A, +)$ možno vzťah (6) prepísať v tvare

$$x + \delta_{i+1} \circ \delta_i^{-1}(y) \neq y + \delta_{i+1} \circ \delta_i^{-1}(x),$$

odkiaľ máme nasledujúci dôsledok:

Dôsledok. *Kód $\mathcal{K}$ s kontrolným znakom nad Abelovou grupou $\mathbb{G} = (A, +)$ objavuje zámenu ľubovoľných susedných znakov na miestach i, $i+1$ práve vtedy, keď pre ľubovoľné x, $y \in A$, $x \neq y$ platí:*

$$x - \delta_{i+1} \circ \delta_i^{-1}(x) \neq y - \delta_{i+1} \circ \delta_i^{-1}(y), \tag{7}$$

t. j. ak zobrazenie $x \mapsto x - \delta_{i+1} \circ \delta_i^{-1}(x)$ je **permutácia**.

Kódy s kontrolným znakom nad grupou – 2

Veta (1.)

Aby kód $\mathcal{K}$ s kontrolným znakom nad grupou $\mathbb{G} = (A, *)$ rozpoznal zámenu ľubovoľných susedných znakov na miestach i, $i+1$ je nevyhnutné a stačí, aby

$$x * \delta_{i+1} \circ \delta_i^{-1}(y) \neq y * \delta_{i+1} \circ \delta_i^{-1}(x) \tag{6}$$

pre všetky $x \in A$, $y \in A$, $x \neq y$.

Pre Abelovu grupu $\mathbb{G} = (A, +)$ možno vzťah (6) prepísať v tvare

$$x + \delta_{i+1} \circ \delta_i^{-1}(y) \neq y + \delta_{i+1} \circ \delta_i^{-1}(x),$$

odkiaľ máme nasledujúci dôsledok:

Dôsledok. *Kód $\mathcal{K}$ s kontrolným znakom nad Abelovou grupou $\mathbb{G} = (A, +)$ objavuje zámenu ľubovoľných susedných znakov na miestach i, $i+1$ práve vtedy, keď pre ľubovoľné x, $y \in A$, $x \neq y$ platí:*

$$x - \delta_{i+1} \circ \delta_i^{-1}(x) \neq y - \delta_{i+1} \circ \delta_i^{-1}(y), \tag{7}$$

t. j. ak zobrazenie $x \mapsto x - \delta_{i+1} \circ \delta_i^{-1}(x)$ je **permutácia**.

Kódy s kontrolným znakom nad grupou – 2

Veta (1.)

Aby kód $\mathcal{K}$ s kontrolným znakom nad grupou $\mathbb{G} = (A, *)$ rozpoznal zámenu ľubovoľných susedných znakov na miestach i, $i+1$ je nevyhnutné a stačí, aby

$$x * \delta_{i+1} \circ \delta_i^{-1}(y) \neq y * \delta_{i+1} \circ \delta_i^{-1}(x) \tag{6}$$

pre všetky $x \in A$, $y \in A$, $x \neq y$.

Pre Abelovu grupu $\mathbb{G} = (A, +)$ možno vzťah (6) prepísať v tvare

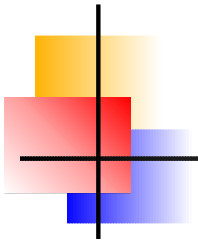
$$x + \delta_{i+1} \circ \delta_i^{-1}(y) \neq y + \delta_{i+1} \circ \delta_i^{-1}(x),$$

odkiaľ máme nasledujúci dôsledok:

Dôsledok. *Kód $\mathcal{K}$ s kontrolným znakom nad Abelovou grupou $\mathbb{G} = (A, +)$ objavuje zámenu ľubovoľných susedných znakov na miestach i, $i+1$ práve vtedy, keď pre ľubovoľné x, $y \in A$, $x \neq y$ platí:*

$$x - \delta_{i+1} \circ \delta_i^{-1}(x) \neq y - \delta_{i+1} \circ \delta_i^{-1}(y), \tag{7}$$

t. j. ak zobrazenie $x \mapsto x - \delta_{i+1} \circ \delta_i^{-1}(x)$ je **permutácia**.



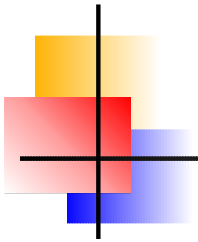
Kódy s kontrolným znakom nad grupou – 3

Nech kód $\mathcal{K}$ rozpoznáva susednú zámenu na miestach i, $i+1$. Potom pre ľubovoľné a_i, a_{i+1} také, že $a_i \neq a_{i+1}$ platí:

$$\underbrace{\delta_i(a_i)}_{x} * \delta_{i+1}(a_{i+1}) \neq \underbrace{\delta_i(a_{i+1})}_{y} * \delta_{i+1}(a_i) \tag{8}$$

$$\underbrace{\delta_i(a_i)}_{x} * \delta_{i+1}(\underbrace{a_{i+1}}_{\delta_i^{-1}(y)}) \neq \underbrace{\delta_i(a_{i+1})}_{y} * \delta_{i+1}(\underbrace{a_i}_{\delta_i^{-1}(x)}) \tag{9}$$

$$x * \delta_{i+1} \circ \delta_i^{-1}(y) \neq y * \delta_{i+1} \circ \delta_i^{-1}(x) \tag{10}$$



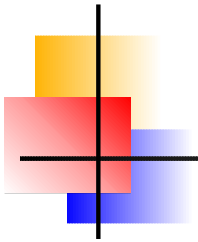
Kódy s kontrolným znakom nad grupou – 3

Nech kód $\mathcal{K}$ rozpoznáva susednú zámenu na miestach i, $i+1$. Potom pre ľubovoľné a_i, a_{i+1} také, že $a_i \neq a_{i+1}$ platí:

$$\underbrace{\delta_i(a_i)}_{x} * \delta_{i+1}(a_{i+1}) \neq \underbrace{\delta_i(a_{i+1})}_{y} * \delta_{i+1}(a_i) \tag{8}$$

$$\underbrace{\delta_i(a_i)}_{x} * \delta_{i+1}(\underbrace{a_{i+1}}_{\delta_i^{-1}(y)}) \neq \underbrace{\delta_i(a_{i+1})}_{y} * \delta_{i+1}(\underbrace{a_i}_{\delta_i^{-1}(x)}) \tag{9}$$

$$x * \delta_{i+1} \circ \delta_i^{-1}(y) \neq y * \delta_{i+1} \circ \delta_i^{-1}(x) \tag{10}$$



Kódy s kontrolným znakom nad grupou – 3

Nech kód $\mathcal{K}$ rozpoznáva susednú zámenu na miestach i, $i+1$. Potom pre ľubovoľné a_i, a_{i+1} také, že $a_i \neq a_{i+1}$ platí:

$$\underbrace{\delta_i(a_i)}_{x} * \delta_{i+1}(a_{i+1}) \neq \underbrace{\delta_i(a_{i+1})}_{y} * \delta_{i+1}(a_i) \tag{8}$$

$$\underbrace{\delta_i(a_i)}_{x} * \delta_{i+1}(\underbrace{a_{i+1}}_{\delta_i^{-1}(y)}) \neq \underbrace{\delta_i(a_{i+1})}_{y} * \delta_{i+1}(\underbrace{a_i}_{\delta_i^{-1}(x)}) \tag{9}$$

$$x * \delta_{i+1} \circ \delta_i^{-1}(y) \neq y * \delta_{i+1} \circ \delta_i^{-1}(x) \tag{10}$$

Kódy s kontrolným znakom nad grupou – 4

Definícia

Permutácia δ (multiplikatívnej) grupy $\mathbb{G} = (A, *)$ sa nazýva **úplným zobrazením**, *ak zobrazenie definované vzťahom*

$$\forall x \in A \quad x \mapsto \eta(x) = x * \delta(x)$$

je zase permutácia.

Permutácia δ (aditívnej) grupy $\mathbb{G} = (A, +)$ sa nazýva **úplným zobrazením**, *ak ak zobrazenie definované vzťahom*

$$\forall x \in A \quad x \mapsto \eta(x) = x + \delta(x)$$

je zase permutácia.

Veta (2.)

Kód $\mathcal{K}$ s kontrolným znakom nad Abelovou grupou $\mathbb{G} = (A, +)$ objavujúci jednoduché chyby a susedné zámeny existuje práve vtedy, keď existuje úplné zobrazenie grupy $\mathbb{G}$.

Kódy s kontrolným znakom nad grupou – 4

Definícia

Permutácia δ (multiplikatívnej) grupy $\mathbb{G} = (A, *)$ sa nazýva **úplným zobrazením**, *ak zobrazenie definované vzťahom*

$$\forall x \in A \quad x \mapsto \eta(x) = x * \delta(x)$$

je zase permutácia.

Permutácia δ (aditívnej) grupy $\mathbb{G} = (A, +)$ sa nazýva **úplným zobrazením**, *ak ak zobrazenie definované vzťahom*

$$\forall x \in A \quad x \mapsto \eta(x) = x + \delta(x)$$

je zase permutácia.

Veta (2.)

Kód $\mathcal{K}$ s kontrolným znakom nad Abelovou grupou $\mathbb{G} = (A, +)$ objavujúci jednoduché chyby a susedné zámeny existuje práve vtedy, keď existuje úplné zobrazenie grupy $\mathbb{G}$.

Kódy s kontrolným znakom nad grupou – 5

Nech kód $\mathcal{K}$ s kontrolnou rovnicou $\sum_{i=1}^{n} \delta_i(a_i)$ objavuje susedné zámeny, potom je zobrazenie

$$x \mapsto \left(x - \delta_{i+1} \circ \delta_i^{-1}(x)\right)$$

permutáciou.

$$x - \delta_{i+1} \circ \delta_i^{-1}(x) = x + \underbrace{[-\delta_{i+1} \circ \delta_i^{-1}(x)]}_{\delta(x)} = x + \delta(x)$$

Permutácia δ definovaná predpisom $\delta = -\delta_{i+1} \circ \delta_i^{-1}$ je hľadaným úplným zobrazením.

Nech existuje úplné zobrazenie δ grupy $\mathbb{G}$. Definujme

$$\delta_i = (-\delta)^i. \tag{11}$$

Potom

$$x - \delta_{i+1} \circ \delta_i^{-1}(x) = x - (-\delta)^{i+1} \circ (-\delta)^{-i}(x) = x - (-\delta)(x) = x + \delta(x),$$

z čoho vyplýva, že $x - \delta_{i+1} \circ \delta_i^{-1}(x)$ je permutácia.
Kód s kontrolným znakom nad grupou $\mathbb{G}$ s permutáciami δ_i definovanými v (11) objavuje susedné zámeny.

Kódy s kontrolným znakom nad grupou – 5

Nech kód $\mathcal{K}$ s kontrolnou rovnicou $\sum_{i=1}^{n} \delta_i(a_i)$ objavuje susedné zámeny, potom je zobrazenie

$$x \mapsto \left(x - \delta_{i+1} \circ \delta_i^{-1}(x)\right)$$

permutáciou.

$$x - \delta_{i+1} \circ \delta_i^{-1}(x) = x + \underbrace{[-\delta_{i+1} \circ \delta_i^{-1}(x)]}_{\delta(x)} = x + \delta(x)$$

Permutácia δ definovaná predpisom $\delta = -\delta_{i+1} \circ \delta_i^{-1}$ je hľadaným úplným zobrazením.

Nech existuje úplné zobrazenie δ grupy $\mathbb{G}$. Definujme

$$\delta_i = (-\delta)^i. \tag{11}$$

Potom

$$x - \delta_{i+1} \circ \delta_i^{-1}(x) = x - (-\delta)^{i+1} \circ (-\delta)^{-i}(x) = x - (-\delta)(x) = x + \delta(x),$$

z čoho vyplýva, že $x - \delta_{i+1} \circ \delta_i^{-1}(x)$ je permutácia.

Kód s kontrolným znakom nad grupou $\mathbb{G}$ s permutáciami δ_i definovanými v (11) objavuje susedné zámeny.

Kódy s kontrolným znakom nad grupou - 6

Veta (3.)

Nech $\mathbb{G}$ je Abelova konečná grupa.
Potom platí:(pozri Codierungstheorie, Eine Einfuhrung, Vieweg, Wiesbaden 1991, ISBN 3-528-06419-6, 8.11 str. 63):

a) *Ak je $\mathbb{G}$ grupa nepárneho rádu, potom je identita na $\mathbb{G}$ úplným zobrazením.*

b) *Grupa $\mathbb{G}$ rádu $r = 2.m$, kde m je nepárne číslo, nemá žiadne úplné zobrazenie*

c) *Nech $\mathbb{G} = (A, +)$ je Abelova grupa párneho rádu. Potom na $\mathbb{G}$ existuje úplné zobrazenie práve vtedy, keď grupa obsahuje aspoň dve rôzne involúcie, t. j. také prvky $g \in A$, že $g \neq 0$, a $g + g = 0$*

Dôsledok

Grupa s nosičom $A = \{0, 1, \ldots, 9\}$ je rádu 2.5 a teda podľa b) nemá žiadne úplné zobrazenie. Neexistuje žiaden dekadický kód s kontrolným znakom nad Abelovou grupou $\mathbb{G} = (A, \oplus)$, ktorý by objavoval jednoduché chyby a susedné zámeny.Jedinou nádejou je použiť kód s kontrolným znakom nad nekomutatívnou grupou.

Kódy s kontrolným znakom nad grupou - 6

Veta (3.)

Nech $\mathbb{G}$ je Abelova konečná grupa.
Potom platí:(pozri Codierungstheorie, Eine Einfuhrung, Vieweg, Wiesbaden 1991, ISBN 3-528-06419-6, 8.11 str. 63):

a) *Ak je $\mathbb{G}$ grupa nepárneho rádu, potom je identita na $\mathbb{G}$ úplným zobrazením.*

b) *Grupa $\mathbb{G}$ rádu $r = 2.m$, kde m je nepárne číslo, nemá žiadne úplné zobrazenie*

c) *Nech $\mathbb{G} = (A, +)$ je Abelova grupa párneho rádu. Potom na $\mathbb{G}$ existuje úplné zobrazenie práve vtedy, keď grupa obsahuje aspoň dve rôzne involúcie, t. j. také prvky $g \in A$, že $g \neq 0$, a $g + g = 0$*

Dôsledok

Grupa s nosičom $A = \{0, 1, \ldots, 9\}$ je rádu 2.5 a teda podľa b) nemá žiadne úplné zobrazenie. Neexistuje žiaden dekadický kód s kontrolným znakom nad Abelovou grupou $\mathbb{G} = (A, \oplus)$, ktorý by objavoval jednoduché chyby a susedné zámeny.Jedinou nádejou je použiť kód s kontrolným znakom nad nekomutatívnou grupou.

Diedrická grupa

Definícia

Diedrická grupa $\mathbb{D}_n$ *je konečná grupa rádu* $2.n$ *tvaru*

$$\{1, a, a^2, \ldots, a^{n-1}, b, ab, a^2.b, \ldots, a^{n-1}b\},$$

kde platí

$$a^n = 1 \quad (a^i \neq 1 \text{ pre } i = 1, 2, \ldots, n-1$$
$$b^2 = 1 \quad (b \neq 1)$$
$$b.a = a^{n-1}.b$$

Diedrickú grupu $\mathbb{D}_n$ *budeme značiť*

$$\mathbb{D}_n = \langle a, b \mid a^n = 1 = b^2,\ ba = a^{n-1}b \rangle$$

Príklad

Diedrická grupa $\mathbb{D}_5 = \langle a, b \mid a^5 = 1 = b^2,\ ba = a^4 b \rangle$. *Prvky grupy* $\mathbb{D}_5$ *možno priradiť dekadickým znakom nasledovne:*

1	a	a^2	a^3	a^4	b	ab	a^2b	a^3b	a^4b
0	1	2	3	4	5	6	7	8	9

Diedrická grupa

Definícia

Diedrická grupa $\mathbb{D}_n$ *je konečná grupa rádu* $2.n$ *tvaru*

$$\{1, a, a^2, \ldots, a^{n-1}, b, ab, a^2.b, \ldots, a^{n-1}b\},$$

kde platí

$$a^n = 1 \quad (a^i \neq 1 \text{ pre } i = 1, 2, \ldots, n-1$$
$$b^2 = 1 \quad (b \neq 1)$$
$$b.a = a^{n-1}.b$$

Diedrickú grupu $\mathbb{D}_n$ *budeme značiť*

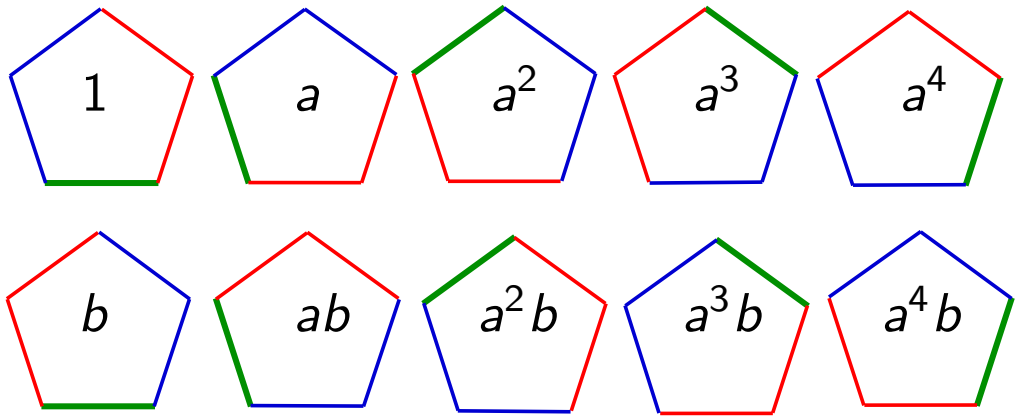
$$\mathbb{D}_n = \langle a, b \mid a^n = 1 = b^2,\ ba = a^{n-1}b \rangle$$

Príklad

Diedrická grupa $\mathbb{D}_5 = \langle a, b \mid a^5 = 1 = b^2,\ ba = a^4 b \rangle$. *Prvky grupy* $\mathbb{D}_5$ *možno priradiť dekadickým znakom nasledovne:*

1	a	a^2	a^3	a^4	b	ab	a^2b	a^3b	a^4b
0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*

Diedrická grupa



Veta (4.)

Nech $\mathbb{D}_n = \langle a, b \mid a^n = 1 = b^2,\ ba = a^{n-1}b \rangle$ *je diedrická grupa nepárneho rádu* n, $n \geq 3$. *Definujme permutáciu* $\delta : \mathbb{D}_n \to \mathbb{D}_n$ *predpisom*

$$\delta(a^i) = a^{n-1-i} \quad a \quad \delta(a^i b) = a^i b \quad \forall i = 0, 1, 2, \ldots, n-1 \ .$$

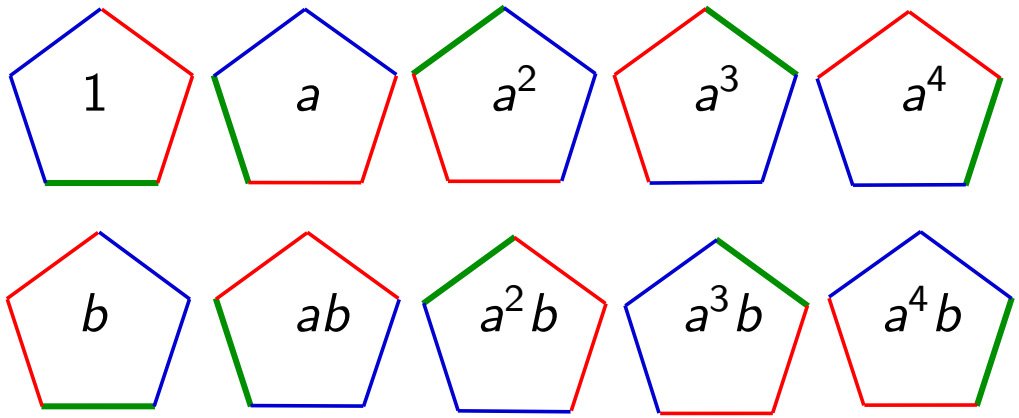
Potom pre permutáciu δ *platí:*

$$x.\delta(y) \neq y.\delta(x) \quad \forall x, y \in \mathbb{D}_n \text{ také, že } x \neq y \ .$$

Dôkaz sa vykoná vyskúšaním týchto možností:

$x = a^i,\ y = a^j$ $\qquad$ $x = a^i b,\ y = a^j$ $\qquad$ $x = a^i b,\ y = a^j b$

Diedrická grupa



Veta (4.)

Nech $\mathbb{D}_n = \langle a, b \mid a^n = 1 = b^2,\ ba = a^{n-1}b \rangle$ *je diedrická grupa nepárneho rádu* n, $n \geq 3$. *Definujme permutáciu* $\delta : \mathbb{D}_n \to \mathbb{D}_n$ *predpisom*

$$\delta(a^i) = a^{n-1-i} \quad a \quad \delta(a^i b) = a^i b \quad \forall i = 0, 1, 2, \ldots, n-1 \ .$$

Potom pre permutáciu δ *platí:*

$$x.\delta(y) \neq y.\delta(x) \quad \forall x, y \in \mathbb{D}_n \text{ také, že } x \neq y \ .$$

Dôkaz sa vykoná vyskúšaním týchto možností:
$x = a^i,\ y = a^j$ $\qquad$ $x = a^i b,\ y = a^j$ $\qquad$ $x = a^i b,\ y = a^j b$

Diedrická grupa

Veta (5.)

Nech $\mathbb{D}_n = \langle a, b \mid a^n = 1 = b^2,\ ba = a^{n-1}b \rangle$ *je iedrická grupa nepárneho rádu* n, $n \geq 3$. *Nech permutácia* $\delta : \mathbb{D}_n \to \mathbb{D}_n$ *je definovaná predpisom*

$$\delta(a^i) = a^{n-1-i} \quad a \quad \delta(a^i b) = a^i b \quad \forall i = 0, 1, 2, \ldots, n-1 \ .$$

Definujme permutácie $\delta_i = \delta^i$ *pre* $i = 1, 2, \ldots, m$. *Potom blokový kód* $\mathcal{K}$ *dĺžky* m *s kontrolným znakom nad grupou* $\mathbb{D}_n$ *(t. j. s kontrolnou rovnicou* $\prod_{i=1}^{m} \delta_i(a_i) = c$*) objavuje jednoduché chyby a susedné zámeny.*

Podľa vety (1.) stačí ukázať, že pre $x \neq y$ platí

$$x * \delta_{i+1} \circ \delta_i^{-1}(y) \neq y * \delta_{i+1} \circ \delta_i^{-1}(x)$$

Keby pre nejaké $x \neq y$ v poslednom vzťahu platila rovnosť, dosadením za $\delta_i = \delta^i,\ \delta_{i+1} = \delta^{i+1}$ by sme dostali

$$x * \delta^{i+1} \circ \delta^{-i}(y) = y * \delta^{i+1} \circ \delta^{-i}(x)$$
$$x * \delta(y) = y * \delta(x),$$

čo by bolo v spore s vlastnosťami permutácie δ. □

Diedrická grupa

Veta (5.)

Nech $\mathbb{D}_n = \langle a, b \mid a^n = 1 = b^2,\ ba = a^{n-1}b \rangle$ *je iedrická grupa nepárneho rádu* n, $n \geq 3$. *Nech permutácia* $\delta : \mathbb{D}_n \to \mathbb{D}_n$ *je definovaná predpisom*

$$\delta(a^i) = a^{n-1-i} \quad a \quad \delta(a^i b) = a^i b \quad \forall i = 0, 1, 2, \ldots, n-1 \ .$$

Definujme permutácie $\delta_i = \delta^i$ *pre* $i = 1, 2, \ldots, m$. *Potom blokový kód* $\mathcal{K}$ *dĺžky* m *s kontrolným znakom nad grupou* $\mathbb{D}_n$ *(t. j. s kontrolnou rovnicou* $\prod_{i=1}^{m} \delta_i(a_i) = c$*) objavuje jednoduché chyby a susedné zámeny.*

Podľa vety (1.) stačí ukázať, že pre $x \neq y$ platí

$$x * \delta_{i+1} \circ \delta_i^{-1}(y) \neq y * \delta_{i+1} \circ \delta_i^{-1}(x)$$

Keby pre nejaké $x \neq y$ v poslednom vzťahu platila rovnosť, dosadením za $\delta_i = \delta^i,\ \delta_{i+1} = \delta^{i+1}$ by sme dostali

$$x * \delta^{i+1} \circ \delta^{-i}(y) = y * \delta^{i+1} \circ \delta^{-i}(x)$$

$$x * \delta(y) = y * \delta(x),$$

čo by bolo v spore s vlastnosťami permutácie δ. □

Diedrická grupa

Veta (5.)

Nech $\mathbb{D}_n = \langle a, b \mid a^n = 1 = b^2,\ ba = a^{n-1}b \rangle$ *je iedrická grupa nepárneho rádu* n, $n \geq 3$. *Nech permutácia* $\delta : \mathbb{D}_n \to \mathbb{D}_n$ *je definovaná predpisom*

$$\delta(a^i) = a^{n-1-i} \quad a \quad \delta(a^i b) = a^i b \quad \forall i = 0, 1, 2, \ldots, n-1 \ .$$

Definujme permutácie $\delta_i = \delta^i$ *pre* $i = 1, 2, \ldots, m$. *Potom blokový kód* $\mathcal{K}$ *dĺžky* m *s kontrolným znakom nad grupou* $\mathbb{D}_n$ *(t. j. s kontrolnou rovnicou* $\prod_{i=1}^{m} \delta_i(a_i) = c$*) objavuje jednoduché chyby a susedné zámeny.*

Podľa vety (1.) stačí ukázať, že pre $x \neq y$ platí

$$x * \delta_{i+1} \circ \delta_i^{-1}(y) \neq y * \delta_{i+1} \circ \delta_i^{-1}(x)$$

Keby pre nejaké $x \neq y$ v poslednom vzťahu platila rovnosť, dosadením za $\delta_i = \delta^i,\ \delta_{i+1} = \delta^{i+1}$ by sme dostali

$$x * \delta^{i+1} \circ \delta^{-i}(y) = y * \delta^{i+1} \circ \delta^{-i}(x)$$
$$x * \delta(y) = y * \delta(x),$$

čo by bolo v spore s vlastnosťami permutácie δ. □

Diedrická grupa $\mathbb{D}_5 = \langle a, b \mid a^5 = 1 = b^2,\ ba = a^4 b \rangle$

1	a	a^2	a^3	a^4	b	ab	a^2b	a^3b	a^4b
0	1	2	3	4	5	6	7	8	9

$i * j$	$0 \le j \le 4$	$5 \le j \le 9$
$0 \le i \le 4$	$(i + j) \mod 5$	$5 + [(i + j) \mod 5]$
$5 \le i \le 9$	$5 + [(i - j) \mod 5]$	$(i - j) \mod 5$

	$*$	j 0	1	2	3	4	5	6	7	8	9
i	0	0	1	2	3	4	5	6	7	8	9
	1	1	2	3	4	0	6	7	8	9	5
	2	2	3	4	0	1	7	8	9	5	6
	3	3	4	0	1	2	8	9	5	6	7
	4	4	0	1	2	3	9	5	6	7	8
	5	5	9	8	7	6	0	4	3	2	1
	6	6	5	9	8	7	1	0	4	3	2
	7	7	6	5	9	8	2	1	0	4	3
	8	8	7	6	5	9	3	2	1	0	4
	9	9	8	7	6	5	4	3	2	1	0

Permutácie δ_i v $\mathbb{D}_5 = \langle a, b \mid a^5 = 1 = b^2,\ ba = a^4 b \rangle$

x	1 0	a 1	a^2 2	a^3 3	a^4 4	b 5	ab 6	a^2b 7	a^3b 8	a^4b 9
$\delta_1(x) = \delta(x)$	4	3	2	1	0	5	6	7	8	9
$\delta_2(x) = \delta^2(x)$	0	1	2	3	4	5	6	7	8	9
$\delta_3(x) = \delta^3(x)$	4	3	2	1	0	5	6	7	8	9

$\delta(a^i) = a^{n-1-i}$ $\qquad$ $\delta(a^i b) = a^i b$

$\delta \circ \delta(a^i) = \delta(a^{n-1-i}) = a^{n-1-[n-1-i]} = a^i$ $\qquad$ $\delta \circ \delta(a^i b) = \delta(a^i b) = a^i b$

$$\delta_1 = \delta_3 = \cdots = \delta_{11} = \ldots := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 3 & 2 & 1 & 0 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$$

$$\delta_2 = \delta_4 = \cdots = \delta_{12} = \ldots := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$$

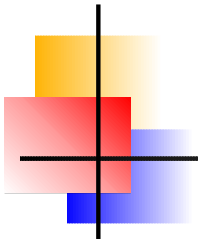
Blokový kód $\mathcal{K}$ dĺžky m s kontrolným znakom nad diedrickou grupou

$$\mathbb{D}_5 = \langle a, b \mid a^5 = 1 = b^2,\ ba = a^4 b \rangle$$

t.j. s kontrolnou rovnicou

$$\prod_{i=1}^{m} \delta_i(a_i) = 0$$

objavuje jednoduché chyby aj susedné zámeny.



THE END

<CTRL/ALT><Del>

Definícia

Guľa $G_t(\mathbf{c})$ **o strede** $\mathbf{c} \in A^n$ **a polomere** t *je množina*

$$G_t(\mathbf{c}) = \{\mathbf{x} \mid \mathbf{x} \in A^n,\ d(\mathbf{x}, \mathbf{c}) \leq t\}.$$

Guľa $G_t(\mathbf{c})$ je množina všetkých takých slov, ktoré vznikli zo slova $\mathbf{c}$ nanajvýš t jednoduchými chybami.

- Samotné slovo $\mathbf{c}$ je tiež prvkom gule $G_t(\mathbf{c})$ a prispieva k počtu jej prvkov číslom $1 = \binom{n}{0}.(r-1)^0$,
- $n.(r-1) = \binom{n}{1}.(r-1)$ – počet slov, ktoré sa líšia od $\mathbf{c} \in A^n$ práve na jednom mieste,
- $\binom{n}{2}.(r-1)^2$ – počet slov, ktoré majú od slova $\mathbf{c}$ vzdialenosť práve 2 je $\binom{n}{2}.(r-1)^2$