

Kombinatorika a grafy I

Martin Balko

13. přednáška

4. ledna 2022



Samoopravné kódy

Připomenutí z minula

Připomenutí z minula

- Přenos dat, vzniklé chyby chceme detekovat a opravit.

Připomenutí z minula

- Přenos dat, vzniklé chyby chceme detekovat a opravit.
- **Abeceda** = množina Σ s q symboly, **slovo** délky n = uspořádaná n -tice symbolů, Σ^n = množina slov délky n nad Σ .

Připomenutí z minula

- Přenos dat, vzniklé chyby chceme detekovat a opravit.
- **Abeceda** = množina Σ s q symboly, **slovo** délky n = uspořádaná n -tice symbolů, Σ^n = množina slov délky n nad Σ .
- **Hammingova vzdálenost** slov $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n) \in \Sigma^n$ je $d(x, y) = |\{i: x_i \neq y_i\}|$.

Připomenutí z minula

- Přenos dat, vzniklé chyby chceme detekovat a opravit.
- **Abeceda** = množina Σ s q symboly, **slovo** délky n = uspořádaná n -tice symbolů, Σ^n = množina slov délky n nad Σ .
- **Hammingova vzdálenost** slov $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n) \in \Sigma^n$ je $d(x, y) = |\{i: x_i \neq y_i\}|$.
- **Kód** = podmnožina $C \subseteq \Sigma^n$ s **kódovými slovy**.

Připomenutí z minula

- Přenos dat, vzniklé chyby chceme detekovat a opravit.
- **Abeceda** = množina Σ s q symboly, **slovo** délky n = uspořádaná n -tice symbolů, Σ^n = množina slov délky n nad Σ .
- **Hammingova vzdálenost** slov $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \Sigma^n$ je $d(x, y) = |\{i: x_i \neq y_i\}|$.
- **Kód** = podmnožina $C \subseteq \Sigma^n$ s **kódovými slovy**.
- V C jsme schopni **opravit $\leq t$ chyby**, pokud pro každé $y \in \Sigma^n$ existuje nanejvýš jedno $x \in C$ s $d(x, y) \leq t$.

Připomenutí z minula

- Přenos dat, vzniklé chyby chceme detekovat a opravit.
- **Abeceda** = množina Σ s q symboly, **slovo** délky n = uspořádaná n -tice symbolů, Σ^n = množina slov délky n nad Σ .
- **Hammingova vzdálenost** slov $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \Sigma^n$ je $d(x, y) = |\{i: x_i \neq y_i\}|$.
- **Kód** = podmnožina $C \subseteq \Sigma^n$ s **kódovými slovy**.
- V C jsme schopni **opravit $\leq t$ chyby**, pokud pro každé $y \in \Sigma^n$ existuje nanejvýš jedno $x \in C$ s $d(x, y) \leq t$.
- **Parametry kódu**: $(n, k, d)_q$, kde $k = \log_q |C|$ a $d = \min_{x \neq y \in C} \{d(x, y)\}$.

Připomenutí z minula

- Přenos dat, vzniklé chyby chceme detekovat a opravit.
- **Abeceda** = množina Σ s q symboly, **slovo** délky n = uspořádaná n -tice symbolů, Σ^n = množina slov délky n nad Σ .
- **Hammingova vzdálenost** slov $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \Sigma^n$ je $d(x, y) = |\{i: x_i \neq y_i\}|$.
- **Kód** = podmnožina $C \subseteq \Sigma^n$ s **kódovými slovy**.
- V C jsme schopni **opravit $\leq t$ chyb**, pokud pro každé $y \in \Sigma^n$ existuje nanejvýš jedno $x \in C$ s $d(x, y) \leq t$.
- **Parametry kódu**: $(n, k, d)_q$, kde $k = \log_q |C|$ a $d = \min_{x \neq y \in C} \{d(x, y)\}$.
- **Příklady kódů**:

Připomenutí z minula

- Přenos dat, vzniklé chyby chceme detekovat a opravit.
- **Abeceda** = množina Σ s q symboly, **slovo** délky n = uspořádaná n -tice symbolů, Σ^n = množina slov délky n nad Σ .
- **Hammingova vzdálenost** slov $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \Sigma^n$ je $d(x, y) = |\{i: x_i \neq y_i\}|$.
- **Kód** = podmnožina $C \subseteq \Sigma^n$ s **kódovými slovy**.
- V C jsme schopni **opravit $\leq t$ chyb**, pokud pro každé $y \in \Sigma^n$ existuje nanejvýš jedno $x \in C$ s $d(x, y) \leq t$.
- **Parametry kódu**: $(n, k, d)_q$, kde $k = \log_q |C|$ a $d = \min_{x \neq y \in C} \{d(x, y)\}$.
- **Příklady kódů**:
 - Opakovací kód $C = \{1 \cdots 1, 2 \cdots 2, \dots, q \cdots q\}$,

Připomenutí z minula

- Přenos dat, vzniklé chyby chceme detekovat a opravit.
- **Abeceda** = množina Σ s q symboly, **slovo** délky n = uspořádaná n -tice symbolů, Σ^n = množina slov délky n nad Σ .
- **Hammingova vzdálenost** slov $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n) \in \Sigma^n$ je $d(x, y) = |\{i: x_i \neq y_i\}|$.
- **Kód** = podmnožina $C \subseteq \Sigma^n$ s **kódovými slovy**.
- V C jsme schopni **opravit $\leq t$ chyb**, pokud pro každé $y \in \Sigma^n$ existuje nanejvýš jedno $x \in C$ s $d(x, y) \leq t$.
- **Parametry kódu**: $(n, k, d)_q$, kde $k = \log_q |C|$ a $d = \min_{x \neq y \in C} \{d(x, y)\}$.
- **Příklady kódů**:
 - Opakovací kód $C = \{1 \cdots 1, 2 \cdots 2, \dots, q \cdots q\}$,
 - kód z Fanovy roviny $C = \{\text{charakteristické vektory přímk}\}$,

Připomenutí z minula

- Přenos dat, vzniklé chyby chceme detekovat a opravit.
- **Abeceda** = množina Σ s q symboly, **slovo** délky n = uspořádaná n -tice symbolů, Σ^n = množina slov délky n nad Σ .
- **Hammingova vzdálenost** slov $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \Sigma^n$ je $d(x, y) = |\{i: x_i \neq y_i\}|$.
- **Kód** = podmnožina $C \subseteq \Sigma^n$ s **kódovými slovy**.
- V C jsme schopni **opravit $\leq t$ chyb**, pokud pro každé $y \in \Sigma^n$ existuje nanejvýš jedno $x \in C$ s $d(x, y) \leq t$.
- **Parametry kódu**: $(n, k, d)_q$, kde $k = \log_q |C|$ a $d = \min_{x \neq y \in C} \{d(x, y)\}$.
- **Příklady kódů**:
 - Opakovací kód $C = \{1 \cdots 1, 2 \cdots 2, \dots, q \cdots q\}$,
 - kód z Fanovy roviny $C = \{\text{charakteristické vektory přímk}\}$,
 - Hadamardův kód $C = \{\text{řádky } H: H \cdot H^T = n \cdot I_n\} \cup \{\text{řádky } -H\}$.

Připomenutí z minula: lineární kódy

Připomenutí z minula: lineární kódy

- **Lineární kód** C je podprostorem vektorového prostoru \mathbb{K}^n , kde $\mathbb{K} \simeq \mathbb{F}_q$ je konečné těleso velikosti q .

Připomenutí z minula: lineární kódy

- **Lineární kód** C je podprostorem vektorového prostoru \mathbb{K}^n , kde $\mathbb{K} \simeq \mathbb{F}_q$ je konečné těleso velikosti q .
- **Parametry**: $[n, k, d]_q$, kde $k = \log_q |C|$ a $d = \min_{x \neq y \in C} \{d(x, y)\}$.

Připomenutí z minula: lineární kódy

- **Lineární kód** C je podprostorem vektorového prostoru \mathbb{K}^n , kde $\mathbb{K} \simeq \mathbb{F}_q$ je konečné těleso velikosti q .
- **Parametry:** $[n, k, d]_q$, kde $k = \log_q |C|$ a $d = \min_{x \neq y \in C} \{d(x, y)\}$.
- Víme, že $|C| = \left| \mathbb{F}_q^{\dim(C)} \right| = q^k$ a $d = \min_{x \in C \setminus \{0\}} d(x, 0)$.

Připomenutí z minula: lineární kódy

- **Lineární kód** C je podprostorem vektorového prostoru \mathbb{K}^n , kde $\mathbb{K} \simeq \mathbb{F}_q$ je konečné těleso velikosti q .
- **Parametry:** $[n, k, d]_q$, kde $k = \log_q |C|$ a $d = \min_{x \neq y \in C} \{d(x, y)\}$.
- Víme, že $|C| = \left| \mathbb{F}_q^{\dim(C)} \right| = q^k$ a $d = \min_{x \in C \setminus \{0\}} d(x, 0)$.
- **Příklady lineárních kódů:**

Připomenutí z minula: lineární kódy

- **Lineární kód** C je podprostorem vektorového prostoru \mathbb{K}^n , kde $\mathbb{K} \simeq \mathbb{F}_q$ je konečné těleso velikosti q .
- **Parametry:** $[n, k, d]_q$, kde $k = \log_q |C|$ a $d = \min_{x \neq y \in C} \{d(x, y)\}$.
- Víme, že $|C| = \left| \mathbb{F}_q^{\dim(C)} \right| = q^k$ a $d = \min_{x \in C \setminus \{0\}} d(x, 0)$.
- **Příklady lineárních kódů:**
 - Opakovací kód je lineární,

Připomenutí z minula: lineární kódy

- **Lineární kód** C je podprostorem vektorového prostoru \mathbb{K}^n , kde $\mathbb{K} \simeq \mathbb{F}_q$ je konečné těleso velikosti q .
- **Parametry:** $[n, k, d]_q$, kde $k = \log_q |C|$ a $d = \min_{x \neq y \in C} \{d(x, y)\}$.
- Víme, že $|C| = \left| \mathbb{F}_q^{\dim(C)} \right| = q^k$ a $d = \min_{x \in C \setminus \{0\}} d(x, 0)$.
- **Příklady lineárních kódů:**
 - Opakovací kód je lineární,
 - kód z Fanovy roviny lineární není, ale jeho rozšíření o $1 \cdots 1$ a doplňky je,

Připomenutí z minula: lineární kódy

- **Lineární kód** C je podprostorem vektorového prostoru \mathbb{K}^n , kde $\mathbb{K} \simeq \mathbb{F}_q$ je konečné těleso velikosti q .
- **Parametry:** $[n, k, d]_q$, kde $k = \log_q |C|$ a $d = \min_{x \neq y \in C} \{d(x, y)\}$.
- Víme, že $|C| = \left| \mathbb{F}_q^{\dim(C)} \right| = q^k$ a $d = \min_{x \in C \setminus \{0\}} d(x, 0)$.
- **Příklady lineárních kódů:**
 - Opakovací kód je lineární,
 - kód z Fanovy roviny lineární není, ale jeho rozšíření o $1 \cdots 1$ a doplňky je,
 - Hadamardův kód obecně lineární není (ale ten ze Sylvesterovy konstrukce je).

Připomenutí z minula: lineární kódy

- **Lineární kód** C je podprostorem vektorového prostoru \mathbb{K}^n , kde $\mathbb{K} \simeq \mathbb{F}_q$ je konečné těleso velikosti q .
- **Parametry:** $[n, k, d]_q$, kde $k = \log_q |C|$ a $d = \min_{x \neq y \in C} \{d(x, y)\}$.
- Víme, že $|C| = \left| \mathbb{F}_q^{\dim(C)} \right| = q^k$ a $d = \min_{x \in C \setminus \{0\}} d(x, 0)$.
- **Příklady lineárních kódů:**
 - Opakovací kód je lineární,
 - kód z Fanovy roviny lineární není, ale jeho rozšíření o $1 \cdots 1$ a doplňky je,
 - Hadamardův kód obecně lineární není (ale ten ze Sylvesterovy konstrukce je).
- S lineárními kódy umíme efektivněji kódovat i dekódovat.

Kód s parametry $[7, 4, 3]_2$ z Fanovy roviny

Kód s parametry $[7, 4, 3]_2$ z Fanovy roviny

- Z Fanovy roviny:

1100001, 0000111, 1010100, 1001010, 0011001, 0101100, 0110010, 1111111
0011110, 1111000, 0101011, 0110101, 1100110, 1010011, 1001101, 0000000

Kód s parametry $[7, 4, 3]_2$ z Fanovy roviny

- Z Fanovy roviny:

1100001, 0000111, 1010100, 1001010, 0011001, 0101100, 0110010, 1111111
0011110, 1111000, 0101011, 0110101, 1100110, 1010011, 1001101, 0000000

- Ekvivalentní kód:

Generující matice:

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Kontrolní matice:

$$M^\perp = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Kód s parametry $[7, 4, 3]_2$ z Fanovy roviny

- Z Fanovy roviny:

1100001, 0000111, 1010100, 1001010, 0011001, 0101100, 0110010, 1111111
0011110, 1111000, 0101011, 0110101, 1100110, 1010011, 1001101, 0000000

- Ekvivalentní kód:

Generující matice:

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Kontrolní matice:

$$M^\perp = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- **Kódování:** $z = (1, 0, 1, 1)^\top \rightarrow x = M^\top z = (1, 0, 1, 1, 1, 0, 0)^\top$.

Kód s parametry $[7, 4, 3]_2$ z Fanovy roviny

- Z Fanovy roviny:

1100001, 0000111, 1010100, 1001010, 0011001, 0101100, 0110010, 1111111
0011110, 1111000, 0101011, 0110101, 1100110, 1010011, 1001101, 0000000

- Ekvivalentní kód:

Generující matice:

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Kontrolní matice:

$$M^\perp = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- **Kódování:** $z = (1, 0, 1, 1)^\top \rightarrow x = M^\top z = (1, 0, 1, 1, 1, 0, 0)^\top$.
- **Dekódování:** $y = (1, 0, 0, 1, 1, 0, 0)^\top \rightarrow s(y) = M^\perp y = (1, 0, 1)^\top$.

Kód s parametry $[7, 4, 3]_2$ z Fanovy roviny

- Z Fanovy roviny:

1100001, 0000111, 1010100, 1001010, 0011001, 0101100, 0110010, 1111111
0011110, 1111000, 0101011, 0110101, 1100110, 1010011, 1001101, 0000000

- Ekvivalentní kód:

Generující matice:

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Kontrolní matice:

$$M^\perp = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- **Kódování:** $z = (1, 0, 1, 1)^\top \rightarrow x = M^\top z = (1, 0, 1, 1, 1, 0, 0)^\top$.
- **Dekódování:** $y = (1, 0, 0, 1, 1, 0, 0)^\top \rightarrow s(y) = M^\perp y = (1, 0, 1)^\top$.
 $s^{-1}(s(y)) = s^{-1}((1, 0, 1)^\top) = (0, 0, 1, 0, 0, 0, 0)^\top \in B(0, 1)$

Kód s parametry $[7, 4, 3]_2$ z Fanovy roviny

- Z Fanovy roviny:

1100001, 0000111, 1010100, 1001010, 0011001, 0101100, 0110010, 1111111
0011110, 1111000, 0101011, 0110101, 1100110, 1010011, 1001101, 0000000

- Ekvivalentní kód:

Generující matice:

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Kontrolní matice:

$$M^\perp = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- **Kódování:** $z = (1, 0, 1, 1)^\top \rightarrow x = M^\top z = (1, 0, 1, 1, 1, 0, 0)^\top$.
- **Dekódování:** $y = (1, 0, 0, 1, 1, 0, 0)^\top \rightarrow s(y) = M^\perp y = (1, 0, 1)^\top$.

$$s^{-1}(s(y)) = s^{-1}((1, 0, 1)^\top) = (0, 0, 1, 0, 0, 0, 0)^\top \in B(0, 1)$$

$$\begin{aligned} x &= y - s^{-1}(s(y)) = (1, 0, 0, 1, 1, 0, 0)^\top - (0, 0, 1, 0, 0, 0, 0)^\top \\ &= (1, 0, 1, 1, 1, 0, 0)^\top \rightarrow z = (1, 0, 1, 1)^\top \end{aligned}$$

Zkoušky

Zkoušky

- Průběh zkoušky:
 - Ústní s písemnou přípravou. Maximálně na 3 hodiny (09:00–12:00, 13:00–16:00 a 16:00–19:00).
 - 5 otázek, z toho 3 na ověření základních pojmů a jejich aplikace, 1 na ověření znalosti důkazů z přednášky a 1 přehledová.

Zkoušky

- Průběh zkoušky:
 - Ústní s písemnou přípravou. Maximálně na 3 hodiny (09:00–12:00, 13:00–16:00 a 16:00–19:00).
 - 5 otázek, z toho 3 na ověření základních pojmů a jejich aplikace, 1 na ověření znalosti důkazů z přednášky a 1 přehledová.
 - Vzorové zadání je na stránkách přednášky.

Zkoušky

- Průběh zkoušky:
 - Ústní s písemnou přípravou. Maximálně na 3 hodiny (09:00–12:00, 13:00–16:00 a 16:00–19:00).
 - 5 otázek, z toho 3 na ověření základních pojmů a jejich aplikace, 1 na ověření znalosti důkazů z přednášky a 1 přehledová.
 - Vzorové zadání je na stránkách přednášky.
 - Během termínů, kdy nebudu zkoušet já, se podmínky mohou lišit!

Zkoušky

- Průběh zkoušky:
 - Ústní s písemnou přípravou. Maximálně na 3 hodiny (09:00–12:00, 13:00–16:00 a 16:00–19:00).
 - 5 otázek, z toho 3 na ověření základních pojmů a jejich aplikace, 1 na ověření znalosti důkazů z přednášky a 1 přehledová.
 - Vzorové zadání je na stránkách přednášky.
 - Během termínů, kdy nebudu zkoušet já, se podmínky mohou lišit!
- Termíny jsou již v SISu.

Zkoušky

- **Průběh zkoušky:**
 - Ústní s písemnou přípravou. Maximálně na 3 hodiny (09:00–12:00, 13:00–16:00 a 16:00–19:00).
 - **5 otázek**, z toho 3 na ověření základních pojmů a jejich aplikace, 1 na ověření znalosti důkazů z přednášky a 1 přehledová.
 - Vzorové zadání je na stránkách přednášky.
 - **Během termínů, kdy nebudu zkoušet já, se podmínky mohou lišit!**
- Termíny jsou již v SISu.
- **Rozsah:** vše, co jsme probrali (viz rozpis jednotlivých přednášek).



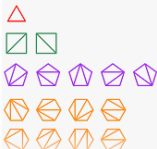


$$|x|! \approx \sqrt{2\pi x} \left(\frac{x}{e}\right)^x$$

Odhady
faktoriálu

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]$$

$$C_n = \frac{1}{n+1} \binom{2n}{n} \text{ pro } n \geq 0.$$



Vytvořující
funkce



Konečné
projektivní
roviny

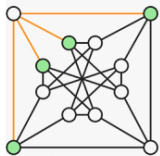
SCIENTIFIC
AMERICAN



Latinské
čtverce



Toky v
sítích



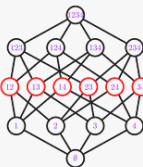
$$k_p(\text{Chvátal}) = 4$$

$$k_n(\text{Chvátal}) = 4$$

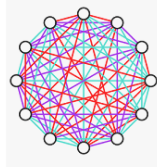
Grafová
souvislost



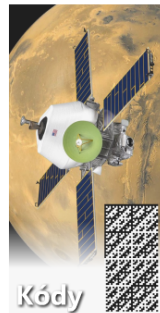
Počet
koster



Spernerova
věta



Ramseyova
teorie



Kódy

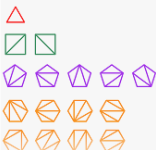


$$|x|! \text{ a } \sqrt{2\pi x} \left(\frac{x}{e}\right)^x.$$

Odhady
faktoriálu

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]$$

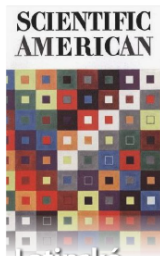
$$C_n = \frac{1}{n+1} \binom{2n}{n} \text{ pro } n \geq 0.$$



Vytvořující
funkce



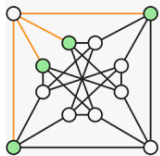
Konečné
projektivní
roviny



Latinské
čtverce



Toky v
sítích



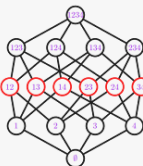
$$k_c(\text{Chvátal}) = 4$$

$$k_v(\text{Chvátal}) = 4$$

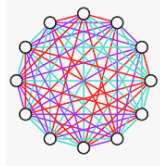
Grafová
souvislost



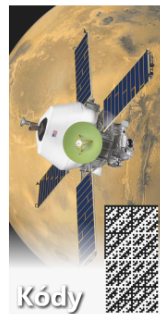
Počet
koster



Spernerova
věta



Ramseyova
teorie



Kódy

Děkuji za pozornost a přeji hodně štěstí u zkoušek.