# Kombinatorika a grafy 1

Martin Balko

## 13. přednáška

4. ledna 2023

# 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 $\Sigma$ s $q$ symboly, slovo délky $n$ $=$ uspořádaná $n$-tice symbolů, $\Sigma^n$ $=$ množina slov délky $n$ nad $\Sigma$.

# Připomenutí z minula

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

# Připomenutí z minula

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

# Připomenutí z minula

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

# Připomenutí z minula

- Přenos dat, vzniklé chyby chceme detekovat a opravit.
- Abeceda = množina $\Sigma$ s $q$ symboly, slovo délky $n$ = uspořádaná $n$-tice symbolů, $\Sigma^n$ = množina slov délky $n$ nad $\Sigma$.
- Hammingova vzdálenost slov $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \Sigma^n$ 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 $d = \min_{x \neq y \in C}\{d(x, y)\}$.

# Připomenutí z minula

- Přenos dat, vzniklé chyby chceme detekovat a opravit.
- Abeceda = množina $\Sigma$ s $q$ symboly, slovo délky $n$ = uspořádaná $n$-tice symbolů, $\Sigma^n$ = množina slov délky $n$ nad $\Sigma$.
- 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 $\Sigma$ s $q$ symboly, slovo délky $n$ = uspořádaná $n$-tice symbolů, $\Sigma^n$ = množina slov délky $n$ nad $\Sigma$.
- Hammingova vzdálenost slov $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \Sigma^n$ je $d(x, y) = |\{i \colon x_i \neq y_i\}|$.
- 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 $C = \{1 \cdots 1, 2 \cdots 2, \ldots, q \cdots q\}$,

# Připomenutí z minula

- Přenos dat, vzniklé chyby chceme detekovat a opravit.
- Abeceda $=$ množina $\Sigma$ s $q$ symboly, slovo délky $n =$ uspořádaná $n$-tice symbolů, $\Sigma^n =$ množina slov délky $n$ nad $\Sigma$.
- Hammingova vzdálenost slov $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \Sigma^n$ je $d(x, y) = |\{i \colon x_i \neq y_i\}|$.
- 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 $C = \{1 \cdots 1, 2 \cdots 2, \ldots, q \cdots q\}$,
  - kód z Fanovy roviny $C = \{\text{charakteristické vektory přímek}\}$,

# Připomenutí z minula

- Přenos dat, vzniklé chyby chceme detekovat a opravit.
- Abeceda $=$ množina $\Sigma$ s $q$ symboly, slovo délky $n$ $=$ uspořádaná $n$-tice symbolů, $\Sigma^n$ $=$ množina slov délky $n$ nad $\Sigma$.
- Hammingova vzdálenost slov $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \Sigma^n$ je $d(x, y) = |\{i \colon x_i \neq y_i\}|$.
- 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 $C = \{1 \cdots 1, 2 \cdots 2, \ldots, q \cdots q\}$,
  - kód z Fanovy roviny $C = \{$charakteristické vektory přímek$\}$,
  - Hadamardův kód $C = \{$řádky $H \colon H \cdot H^\top = n \cdot I_n\} \cup \{$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 nad $\mathbb{Z}_q$,

# 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 $d = \min_{x \neq y \in C}\{d(x, y)\}$.
- 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 nad $\mathbb{Z}_q$,
    - 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 nad $\mathbb{Z}_q$,
    - 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 nad $\mathbb{Z}_q$,
  - 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.

# Syndrom u kódu s parametry $[5, 2, 3]_2$

# Syndrom u kódu s parametry $[5,2,3]_2$

Generující matice:

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

Kontrolní matice:

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

# Syndrom u kódu s parametry $[5,2,3]_2$

Generující matice:

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

Kontrolní matice:

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

- Tabulka reprezentující $s^{-1}$:

| syndrom $s(y)$ | reprezentant $s^{-1}(s(y))$ | ostatní slova z $\mathbb{F}_2^5$ |
|---|---|---|
| 000 | 00000 | 11100 00111 11011 |
| 001 | 00001 | 11101 00110 11010 |
| 010 | 00100 | 11000 00011 11111 |
| 011 | 00010 | 11001 00101 11110 |
| 100 | 10000 | 01100 10111 01011 |
| 101 | 01010 | 10001 01101 10110 |
| 110 | 01000 | 10100 10011 01111 |
| 111 | 01001 | 10101 10010 01110 |

# 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: $z = (1, 0, 1, 1)^\top \to x = M^\top z = (1, 0, 1, 1, 1, 0, 0)^\top$.

# 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: $z = (1,0,1,1)^{\top} \to x = M^{\top} z = (1,0,1,1,1,0,0)^{\top}$.
- Dekódování: $y = (1,0,0,1,1,0,0)^{\top} \to s(y) = M^{\perp} y = (1,0,1)^{\top}$.

# 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: $z = (1,0,1,1)^{\top} \to x = M^{\top} z = (1,0,1,1,1,0,0)^{\top}$.
- Dekódování: $y = (1,0,0,1,1,0,0)^{\top} \to s(y) = M^{\perp} y = (1,0,1)^{\top}$.

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

# 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: $z = (1,0,1,1)^{\top} \to x = M^{\top} z = (1,0,1,1,1,0,0)^{\top}$.
- Dekódování: $y = (1,0,0,1,1,0,0)^{\top} \to s(y) = M^{\perp} y = (1,0,1)^{\top}$.

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

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

$$= (1,0,1,1,1,0,0)^{\top} \ \to \ z = (1,0,1,1)^{\top}$$

# 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

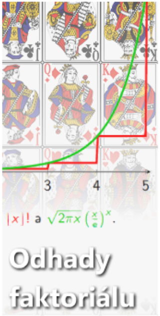
- Průběh zkoušky:
  - Ústní s písemnou přípravou. Maximálně na 3 hodiny (09:00–12:00, 13:00–16:00 a 16:00–19:00).
  - 5 otázek, z toho 3 na ověření základních pojmů a jejich aplikace, 1 na ověření znalosti důkazů z přednášky a 1 přehledová.
  - Vzorové zadání je na stránkách přednášky.

# Zkoušky

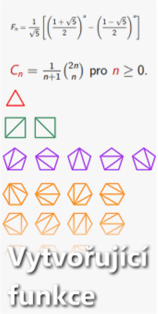
- Průběh zkoušky:
  - Ústní s písemnou přípravou. Maximálně na 3 hodiny (09:00–12:00, 13:00–16:00 a 16:00–19:00).
  - 5 otázek, z toho 3 na ověření základních pojmů a jejich aplikace, 1 na ověření znalosti důkazů z přednášky a 1 přehledová.
  - Vzorové zadání je na stránkách přednášky.
- Termíny jsou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



Odhady faktoriálu

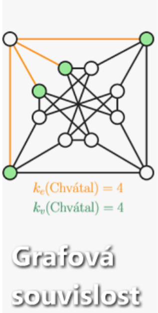


Vytvořující funkce


Konečné projektivní roviny

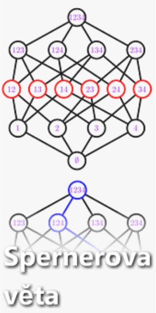
Latinské čtverce

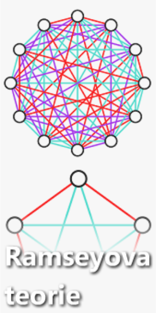

Toky v sítích

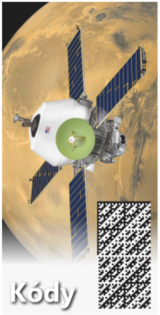


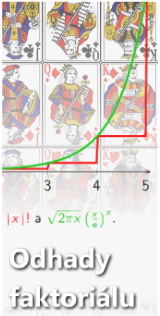
Grafová souvislost

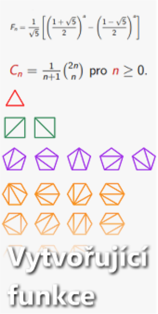

Počet koster


Spernerova věta


Ramseyova teorie

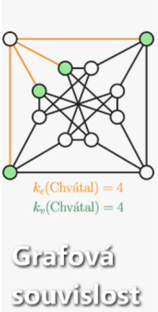

Kódy



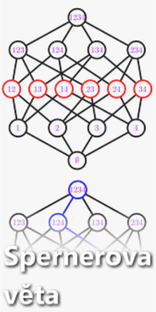



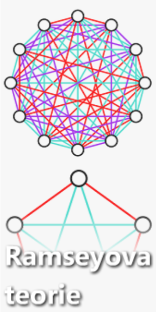


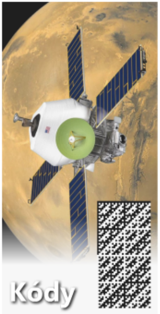









Děkuji za pozornost a přeji hodně štěstí u zkoušek.