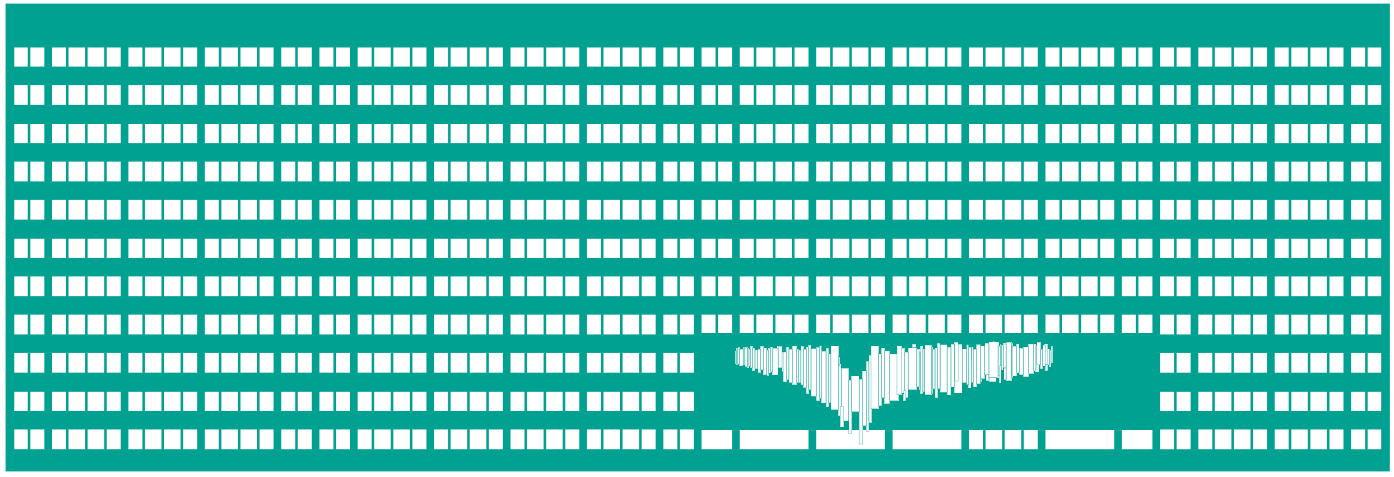
VŠB TECHNICKÁ UNIVERZITA OSTRAVA

VSB TECHNICAL UNIVERSITY OF OSTRAVA



www.vsb.cz

Jak komunikujeme s vesmírnými sondami

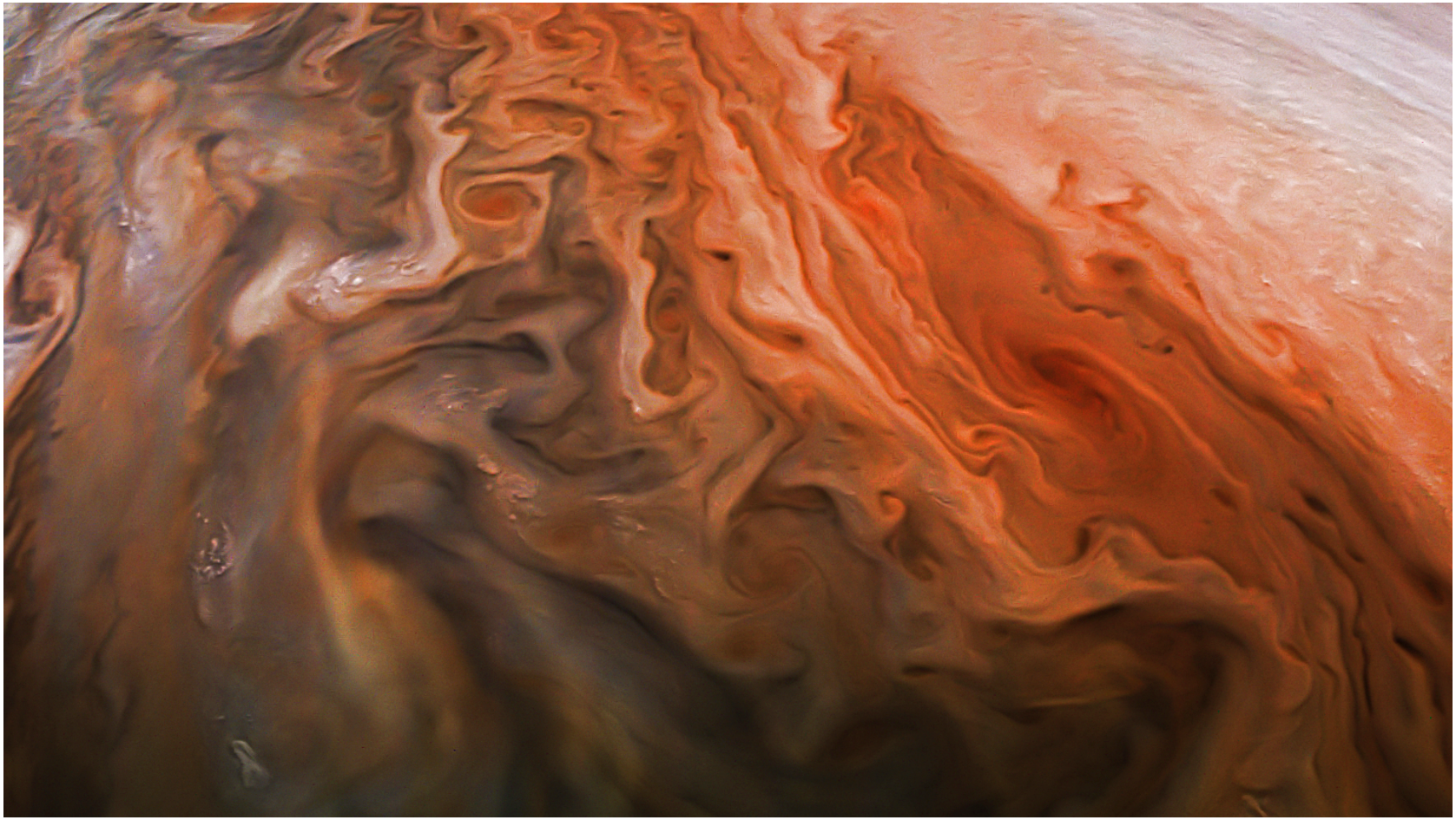
aneb něco málo o samoopravných kódech a algebře

Tereza Kovářová

VŠB – Technická univerzita Ostrava
Katedra aplikované matematiky
tereza.kovarova@vsb.cz

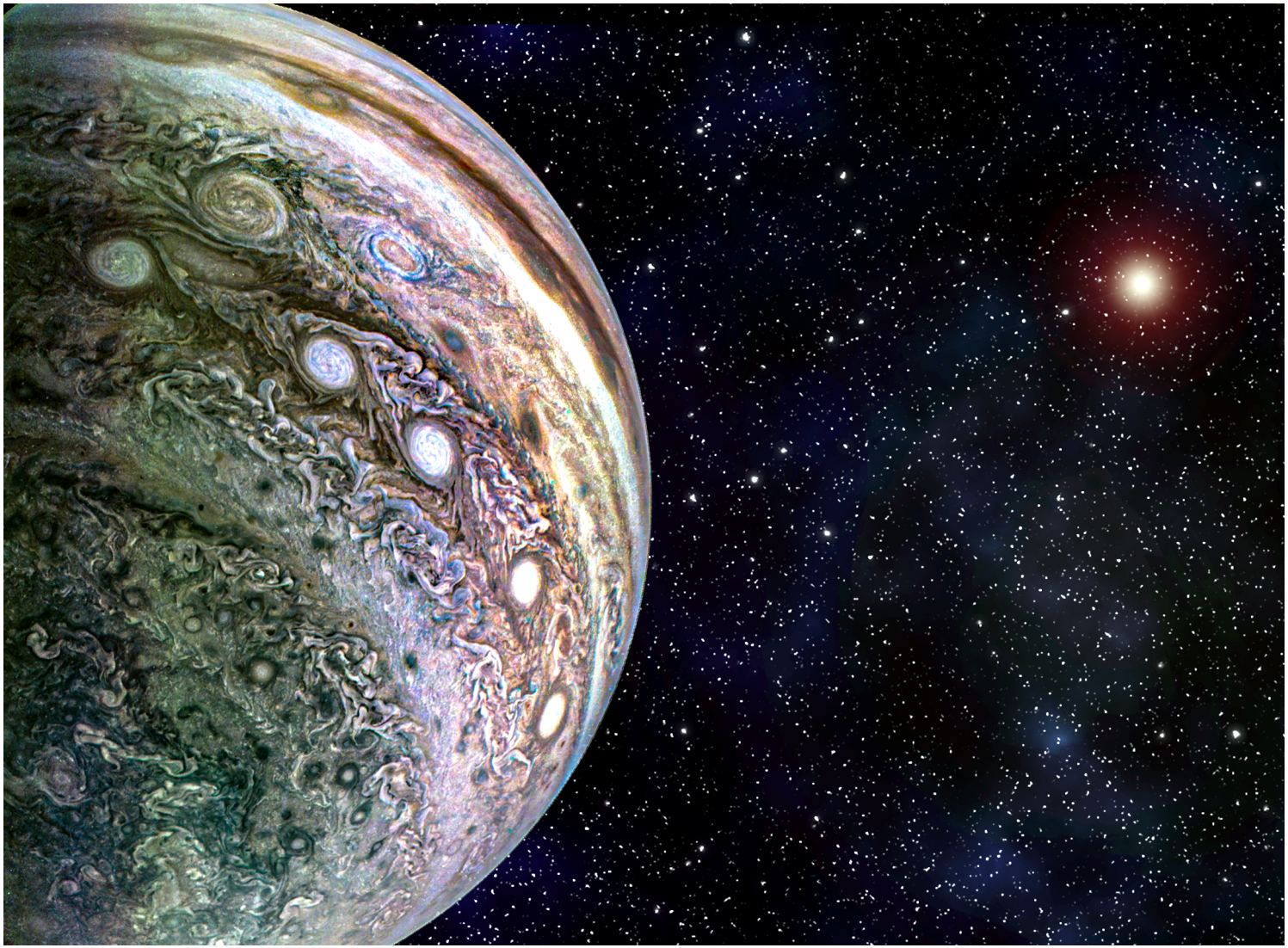
ŠKOMAM 2. 2. 2022, Ostrava

VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA ELEKTROTECHNIKY A INFORMATIKY | KATEDRA APLIKOVANÉ MATEMATIKY

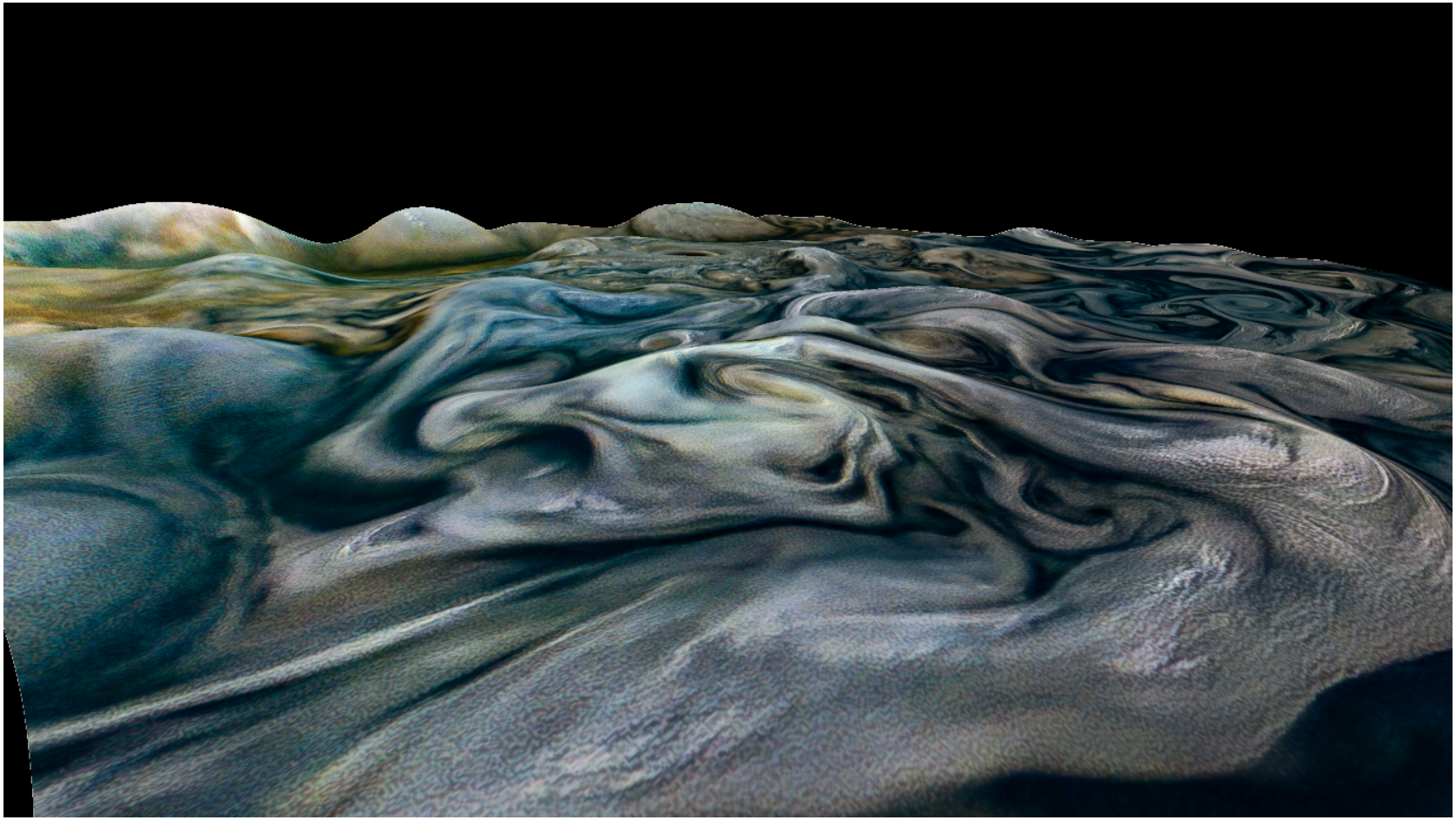


▸ PJ32 Perijove, detail, pretty

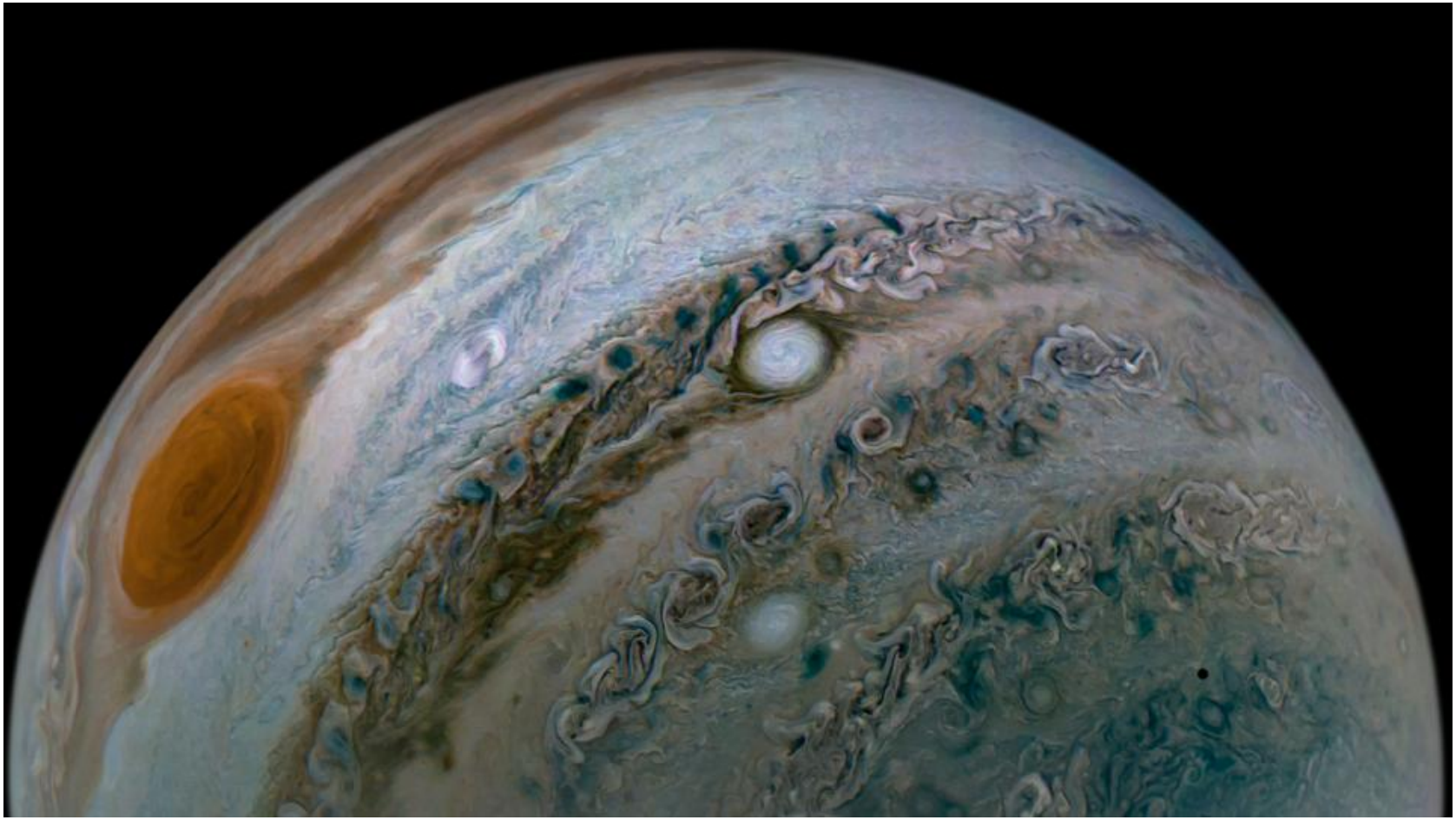
▸ PJ3 image 114: SEB west of Great Red Spot



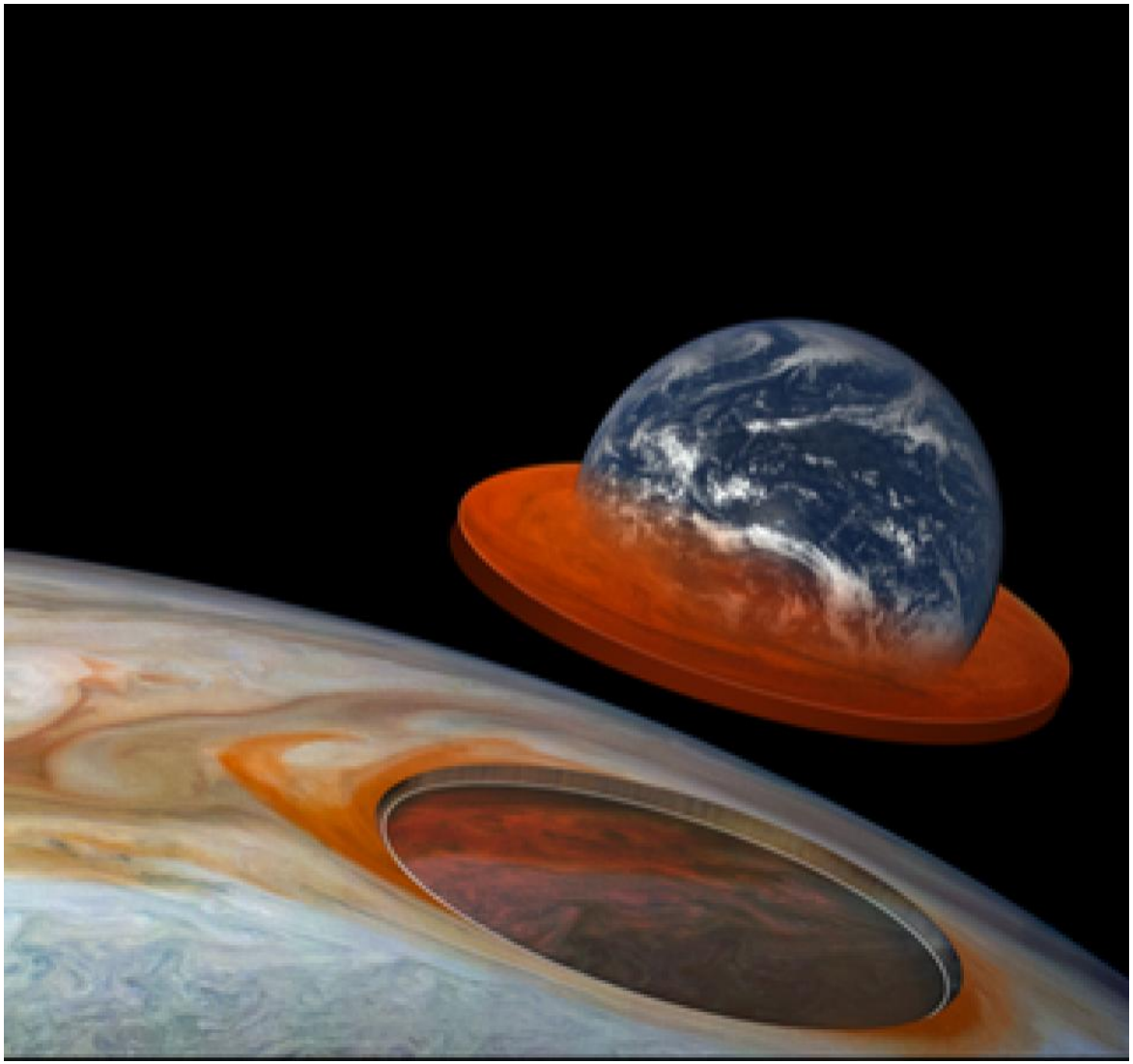
▸ PJ34 Southern Oval Parade



▸ Storm knots



▸ Jupiter - PJ27 JET S4 Domain



▸ Jupiter's Great Red Spot and Earth

▸ Juno above Jupiter

Juno – americká kosmická sonda, NASA program **New Frontiers**

- účel mise – průzkum atmosféry a měsíců planety Jupiter (polární oběžná dráha)
- odstartovala 5. srpna 2011 a 5. července 2016 doletěla k Jupiteru
- první meziplanetární sonda napájená solárními panely
- plánováno 37 oběhů ve 20 měsících
- od prosince 2016 – mise prodloužena do září 2025 nebo zániku sondy

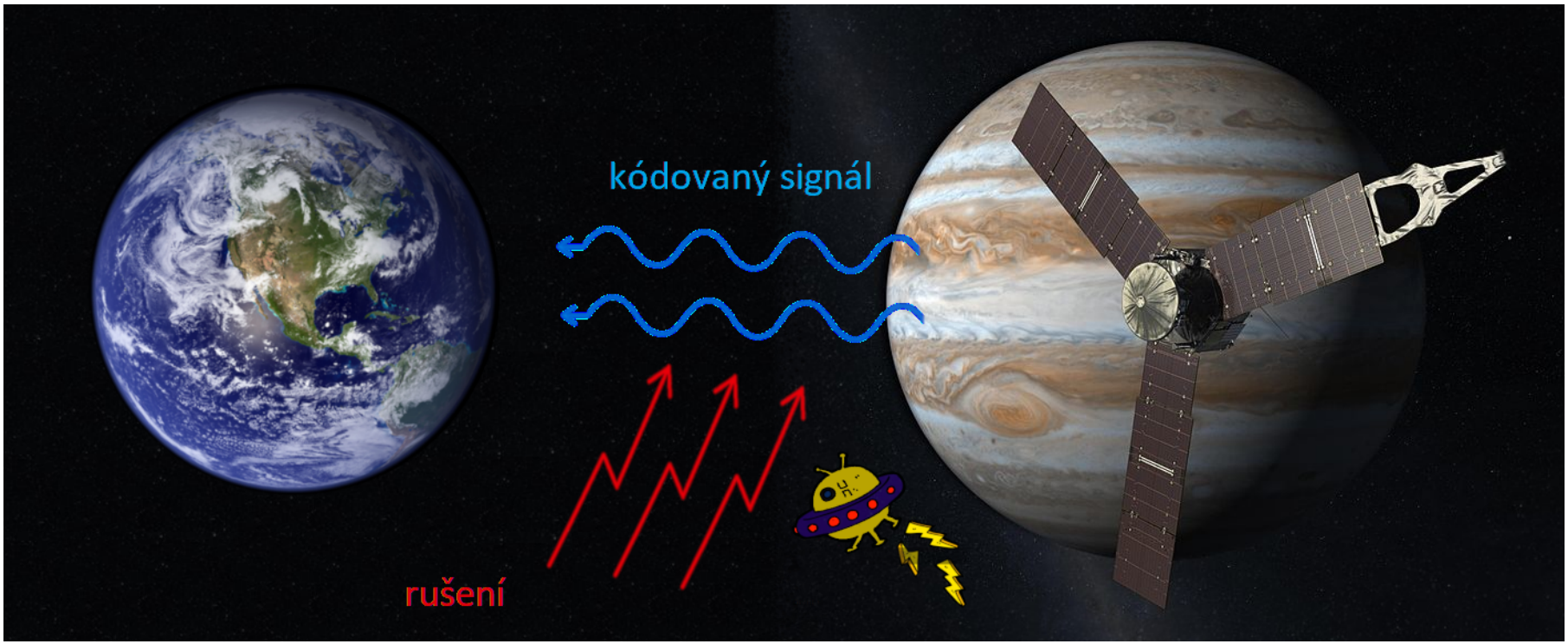
▸ juno-mission-expands-into-the-future

Juno – americká kosmická sonda, NASA program **New Frontiers**

Technické vybavení:

- Solární panely (5,2 AU)
- Mikrovlnný radiometr (MWR)
- Infračervený mapovač polárních září (JIRAM)
- Detektor energetických částic (JEDI)
- Detektor rádiových a plasmatických vln (WAWES)
- Ultrafialový spektrograf (UVS)
- Kamera (UCA)
- Vysokozisková anténa (K_a band)

- sonda Juno – zkoumá atmosféru a měsíce Jupitera
- komunikace se sondou – rušení signálu při přenosu informace



Odolnost Juno proti chybám při přenosu informace

Question:

What techniques have been employed for the Juno spacecraft to successfully transmit data packets back to Earth once she's in a polar orbit around Jupiter? Jupiter is a strong source of radio wavelength interference, at the same time it is of course also rather large distance away from the Earth (currently roughly 5.135 AU).

Answer:

It is a standard deep-space X-band system with a 2.5 m high-gain antenna, a 25 W traveling-wave tube amplifier, and concatenated convolutional and Reed-Solomon or Turbo 1/6 rate error-correcting codes (RS [255,223]-code). It will get 18,000 bits per second down to a 34-m antenna on Earth at maximum range (6.459 AU) at a $10-6$ bit error rate.

Most of the noise in the transmission comes from space plasma between Jupiter and Earth, and Earth's atmosphere. Not from Jupiter. Jupiter is noisy in the MHz frequencies, but not in the GHz frequencies.

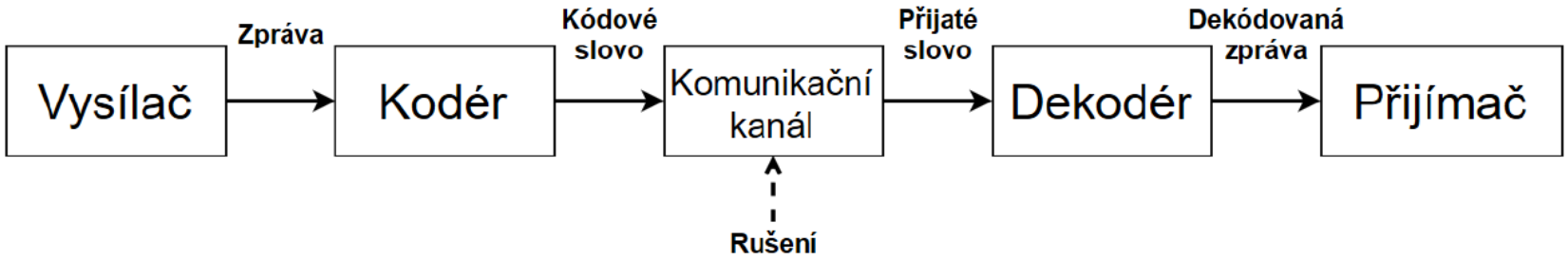
▸ resilience-to-data-transmission-errors-of-the-juno-spacecraft

O čem přednáška bude

- Využití samoopravných kódů
- Základní vlastnosti samoopravných kódů
- Kódování a dekódování pomocí jednoduchého lineárního kódu
- LEGO robot a samoopravný kód

Využití samoopravných kódů

Samoopravné kódy se používají k opravě chyb při přenosu digitální informace zašuměným kanálem.

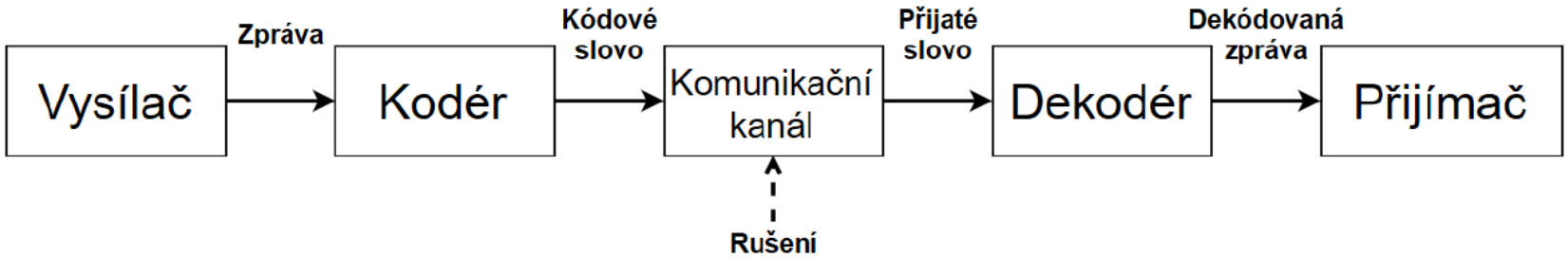


komunikační kanál:
- telefonní komunikační kanály
- linka mezi počítači
- přenos dat v počítači mezi pevným diskem a operační pamětí
- přenos informací v satelitních systémech
- komunikace s vesmírnými sondami
- kompaktní disk
- magnetická páska
- QR-kódy

rušení (šum):
- interference s kosmickým zářením
- sluneční záření
- em-záření v zemské atmosféře
- škrábance na CD
- přehnutí magnetické pásky
- poškození obrázku QR-kódu

Využití samoopravných kódů

Samoopravné kódy se používají k opravě chyb při přenosu digitální informace zašuměným kanálem.

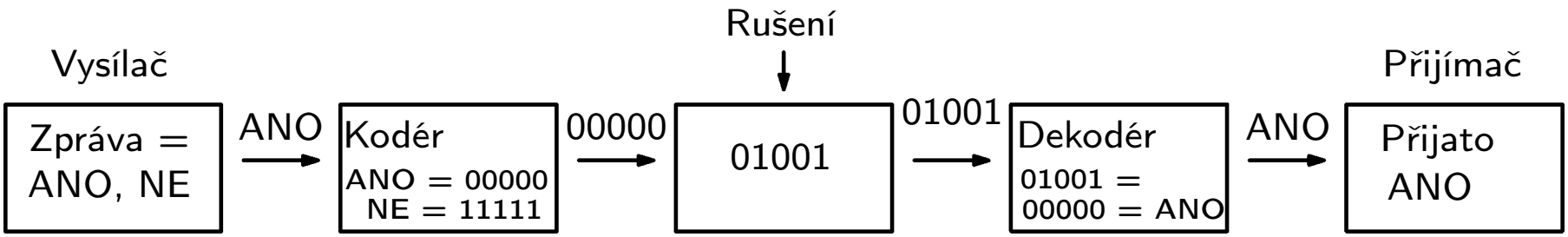


komunikační kanál:
- telefonní komunikační kanály
- linka mezi počítači
- přenos dat v počítači mezi pevným diskem a operační pamětí
- přenos informací v satelitních systémech
- komunikace s vesmírnými sondami
- kompaktní disk
- magnetická páska
- QR-kódy

rušení (šum):
- interference s kosmickým zářením
- sluneční záření
- em-záření v zemské atmosféře
- škrábance na CD
- přehnutí magnetické pásky
- poškození obrázku QR-kódu

Příklady samoopravných kódů

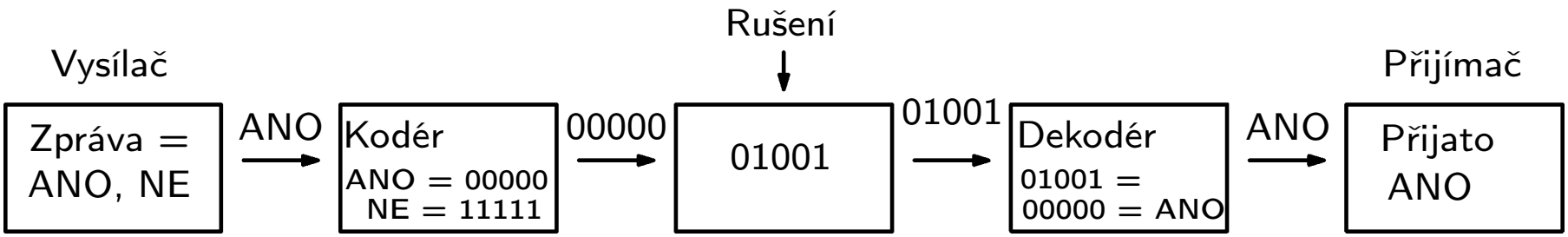
1.) Binární opakovací kód délky 5 je $C = \{00000, 11111\}$



2.) Obecně q-ární kód C:
Blokový q-ární kód délky n je množina uspořádaných n-tic (slov, vektorů, sekvencí) tvořených q navzájem různými symboly zvolené abecedy F_q.
Množinu všech uspořádaných n-tic z q symbolů značíme $(F_q)^n$.
(Často je za F_q voleno konečné těleso $GF(q)$, ke q je mocnina prvočísla.)

Příklady samoopravných kódů

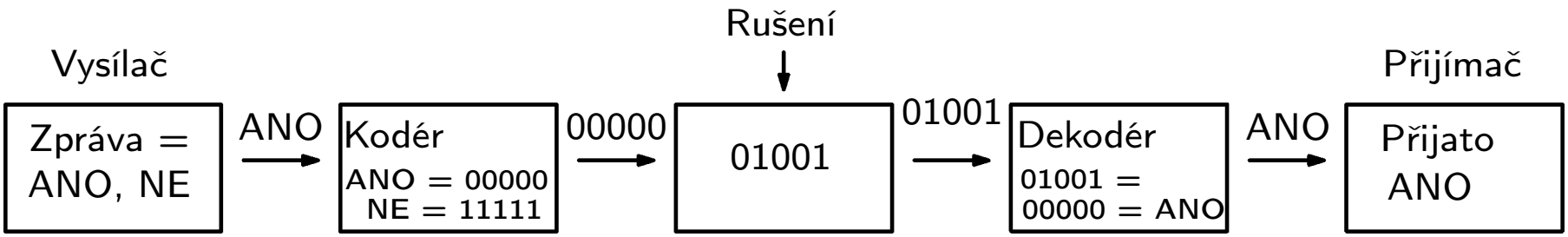
1.) Binární opakovací kód délky 5 je $C = \{00000, 11111\}$



2.) Obecně q-ární kód C:
Blokový q-ární kód délky n je množina uspořádaných n-tic (slov, vektorů, sekvencí) tvořených q navzájem různými symboly zvolené abecedy F_q.
Množinu všech uspořádaných n-tic z q symbolů značíme $(F_q)^n$.
(Často je za F_q voleno konečné těleso $GF(q)$, ke q je mocnina prvočísla.)

Příklady samoopravných kódů

1.) Binární opakovací kód délky 5 je $C = \{00000, 11111\}$



2.) Obecně q-ární kód C:
Blokový q-ární kód délky n je množina uspořádaných n-tic (slov, vektorů, sekvencí) tvořených q navzájem různými symboly zvolené abecedy F_q.
Množinu všech uspořádaných n-tic z q symbolů značíme $(F_q)^n$.
(Často je za F_q voleno konečné těleso $GF(q)$, ke q je mocnina prvočísla.)

Příklady samoopravných kódů

3.) Binární kódy: $C_1 = \{00, 01, 10, 11\}$
$C_2 = \{000, 011, 101, 110\}$
$C_3 = \{00000, 01101, 10110, 11011\}$

$F_q = \{0, 1\}$, $M = |C_1| = |C_2| = |C_3| = 4$, $n_1 = 2$, $n_2 = 3$, $n_3 = 5$

Redundance ovlivňuje, kolik chyb lze detekovat a kolik lze opravit.

Princip fungování

Informace/Pokyn		Detekce		Opravování
00				
01	$\longrightarrow$		$\longrightarrow$	
10				
11				

Příklady samoopravných kódů

3.) Binární kódy: $C_1 = \{00, 01, 10, 11\}$
$C_2 = \{000, 011, 101, 110\}$
$C_3 = \{00000, 01101, 10110, 11011\}$

$F_q = \{0, 1\}$, $M = |C_1| = |C_2| = |C_3| = 4$, $n_1 = 2$, $n_2 = 3$, $n_3 = 5$

Redundance ovlivňuje kolik chyb lze detekovat a kolik lze opravit.

Princip fungování

Informace/Pokyn		Detekce		Opravování
00		000		
01	$\longrightarrow$	011	$\longrightarrow$	
10		101		
11		110		

Příklady samoopravných kódů

3.) Binární kódy: $C_1 = \{00, 01, 10, 11\}$
$C_2 = \{000, 011, 101, 110\}$
$C_3 = \{00000, 01101, 10110, 11011\}$

$F_q = \{0, 1\}$, $M = |C_1| = |C_2| = |C_3| = 4$, $n_1 = 2$, $n_2 = 3$, $n_3 = 5$

Redundance ovlivňuje kolik chyb lze detekovat a kolik lze opravit.

Princip fungování

Informace/Pokyn		Detekce		Opravování
00		000		00000
01	$\longrightarrow$	011	$\longrightarrow$	01101
10		101		10110
11		110		11011

Základní parametry kódu

$C_3 = \{00000, 01101, 10110, 11011\}$

Hammingova vzdálenost

Hammingova vzdálenost dvou kódových slov $d(\mathbf{x}, \mathbf{y})$ je rovna počtu pozic, na kterých se slova $\mathbf{x}$ a $\mathbf{y}$ liší.

$d(01101, 10110) = 4$

Minimální vzdálenost kódu

$d(C) = \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}$

$d(C_3) = 3$

Co je (n, M, d)-kód ?

Kód C s délkou kódových slov n, počtem kódových slov M a minimální vzdáleností $d(C) = d$ se značí (n, M, d)-kód.

Kód C_3 je $(5, 4, 3)$-kód.

Základní parametry kódu

$C_3 = \{00000, 01101, 10110, 11011\}$

Hammingova vzdálenost

Hammingova vzdálenost dvou kódových slov $d(\mathbf{x}, \mathbf{y})$ je rovna počtu pozic, na kterých se slova $\mathbf{x}$ a $\mathbf{y}$ liší.

$d(01101, 10110) = 4$

Minimální vzdálenost kódu

$d(C) = \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}$

$d(C_3) = 3$

Co je (n, M, d)-kód ?

Kód C s délkou kódových slov n, počtem kódových slov M a minimální vzdáleností $d(C) = d$ se značí (n, M, d)-kód.

Kód C_3 je $(5, 4, 3)$-kód.

Základní parametry kódu

$C_3 = \{00000, 01101, 10110, 11011\}$

Hammingova vzdálenost

Hammingova vzdálenost dvou kódových slov $d(\mathbf{x}, \mathbf{y})$ je rovna počtu pozic, na kterých se slova $\mathbf{x}$ a $\mathbf{y}$ liší.

$d(01101, 10110) = 4$

Minimální vzdálenost kódu

$d(C) = \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}$

$d(C_3) = 3$

Co je (n, M, d)-kód ?

Kód C s délkou kódových slov n, počtem kódových slov M a minimální vzdáleností $d(C) = d$ se značí (n, M, d)-kód.

Kód C_3 je $(5, 4, 3)$-kód.

Minnimální vzdálenost a schopnost kódu opravovat chyby

Hammingova vzdálenost je metrikou, tj. má tyto vlastnosti:

(i) $d(\mathbf{x}, \mathbf{y}) = 0$ jestliže $\mathbf{x} = \mathbf{y}$

(ii) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$ pro všechna $\mathbf{x}, \mathbf{y} \in (F_q)^n$

(iii) $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$ pro všechna $\mathbf{x}, \mathbf{y}, \mathbf{z} \in (F_q)^n$

Kód C s minimální vzdáleností $d(C) = d$ lze použít buď k:

(i) detekci až $d - 1$ chyb,

(ii) nebo k opravě až t chyb, kde $2t + 1 \leq d$.

Důkaz: (ii) Přepokládejme, že $d \geq 2t + 1$, a že $\mathbf{x}$ je odeslané slovo a $\mathbf{y}$ je přijaté slovo s t nebo méně chybami, tj $d(\mathbf{x}, \mathbf{y}) \leq t$. Pro kterékoliv jiné slovo $\mathbf{x}'$ je jistě $d(\mathbf{x}', \mathbf{y}) \geq t + 1$. Kdyby bylo $d(\mathbf{x}', \mathbf{y}) \leq t$, dostali bychom, že $d(\mathbf{x}', \mathbf{x}) \leq d(\mathbf{x}', \mathbf{y}) + d(\mathbf{x}, \mathbf{y}) \leq 2t$. Spor s $d \geq 2t + 1$.

Minnimální vzdálenost a schopnost kódu opravovat chyby

Hammingova vzdálenost je metrikou, tj. má tyto vlastnosti:

(i) $d(\mathbf{x}, \mathbf{y}) = 0$ jestliže $\mathbf{x} = \mathbf{y}$

(ii) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$ pro všechna $\mathbf{x}, \mathbf{y} \in (F_q)^n$

(iii) $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$ pro všechna $\mathbf{x}, \mathbf{y}, \mathbf{z} \in (F_q)^n$

Kód C s minimální vzdáleností $d(C) = d$ lze použít buď k:

(i) detekci až $d - 1$ chyb,

(ii) nebo k opravě až t chyb, kde $2t + 1 \leq d$.

Důkaz: (ii) Přepokládejme, že $d \geq 2t + 1$, a že $\mathbf{x}$ je odeslané slovo a $\mathbf{y}$ je přijaté slovo s t nebo méně chybami, tj $d(\mathbf{x}, \mathbf{y}) \leq t$. Pro kterékoliv jiné slovo $\mathbf{x}'$ je jistě $d(\mathbf{x}', \mathbf{y}) \geq t + 1$. Kdyby bylo $d(\mathbf{x}', \mathbf{y}) \leq t$, dostali bychom, že $d(\mathbf{x}', \mathbf{x}) \leq d(\mathbf{x}', \mathbf{y}) + d(\mathbf{x}, \mathbf{y}) \leq 2t$. Spor s $d \geq 2t + 1$.

Co je to „dobrý“ kód?

Dobrý kód umožní:

1. rychlé kódování informace,
2. snadný přenos zakódované zprávy,
3. rychlé dekódování přijaté zprávy,
4. opravu chyb způsobených šumem v kanálu během přenosu zprávy,
5. maximalizaci množství informace přenesené za jednotku času.

Dobrý (n, M, d)-kód má:

- malé n pro snadný/rychlý přenos informace
- velké M pro velkou variabilitu kódovaných informací
- velké d pro možnost opravit co nejvíce chyb

Hlavní problém teorie kódování

Obvykle, pro dané n a d, najít co největší kód, tj. maximalizovat M.

Co je to „dobrý“ kód?

Dobrý kód umožní:

1. rychlé kódování informace,
2. snadný přenos zakódované zprávy,
3. rychlé dekódování přijaté zprávy,
4. opravu chyb způsobených šumem v kanálu během přenosu zprávy,
5. maximalizaci množství informace přenesené za jednotku času.

Dobrý (n, M, d)-kód má:

- malé n pro snadný/rychlý přenos informace
- velké M pro velkou variabilitu kódovaných informací
- velké d pro možnost opravit co nejvíce chyb

Hlavní problém teorie kódování

Obvykle, pro dané n a d, najít co největší kód, tj. maximalizovat M.

Značení

$\max M_q(n,d)$ – maximální počet slov M takový, že existuje q-ární (n,M,d)-kód.

Příklady:

- $\max M_q(n,1) = q^n$ a $\max M_q(n,n) = q$
- $\max M_2(5,3) = ?$

$$C_3 = \begin{cases} 00000 \\ 01101 \\ 10110 \\ 11011 \end{cases}$$ je $(5,4,3)$-kód a tedy $\max M_2(5,3) \geq 4$.

Existuje $(5,5,3)$-kód? (Prověřit přes 200 000 5-prkových podmnožin $(F_2)^5$)

Ukážeme, že $(5,M,3)$-kód musí mít $M \leq 4$ a že C_3 je jediný $(5,4,3)$-kód až na ekvivalenci.

Značení

$\max M_q(n,d)$ – maximální počet slov M takový, že existuje q-ární (n,M,d)-kód.

Příklady:

- $\max M_q(n,1) = q^n$ a $\max M_q(n,n) = q$
- $\max M_2(5,3) = ?$

$$C_3 = \begin{cases} 00000 \\ 01101 \\ 10110 \\ 11011 \end{cases}$$ je $(5,4,3)$-kód a tedy $\max M_2(5,3) \geq 4$.

Existuje $(5,5,3)$-kód? (Prověřit přes 200 000 5-prkových podmnožin $(F_2)^5$)

Ukážeme, že $(5,M,3)$-kód musí mít $M \leq 4$ a že C_3 je jediný $(5,4,3)$-kód až na ekvivalenci.

Značení

$\max M_q(n,d)$ – maximální počet slov M takový, že existuje q-ární (n,M,d)-kód.

Příklady:

- $\max M_q(n,1) = q^n$ a $\max M_q(n,n) = q$
- $\max M_2(5,3) = ?$

$$C_3 = \begin{cases} 00000 \\ 01101 \\ 10110 \\ 11011 \end{cases}$$ je $(5,4,3)$-kód a tedy $\max M_2(5,3) \geq 4$.

Existuje $(5,5,3)$-kód? (Prověřit přes 200 000 5-prkových podmnožin $(F_2)^5$)

Ukážeme, že $(5,M,3)$-kód musí mít $M \leq 4$ a že C_3 je jediný $(5,4,3)$-kód až na ekvivalenci.

$$C_3 = \begin{cases} 00000 \\ 01101 \\ 10110 \\ 11011 \end{cases}$$

Tvrzení:

$(5, M, 3)$-kód C musí mít $M \leq 4$ a C_3 je jediný $(5, 4, 3)$-kód až na ekvivalenci.

Důkaz:
Předpokládejme, že slovo $\mathbf{0} = 00000$ patří kódu C.
Pak C nemůže obsahovat žádná slova s jednou 1, nebo dvěma 1, protože $d = 3$.
C může obsahovat nejvýš jedno slovo se čtyřmi nebo pěti 1. Dvě slova by se lišila na nejvýše dvou pozicích.
C musí obsahovat alespoň dvě slova s třemi 1, protože $M \geq 4$.

$$\begin{matrix} 00000 \\ 11100 \\ 00111 \end{matrix}$$

Čtvrté slovo pak zřejmě musí být:

$$11011$$

$$C_3 = \begin{cases} 00000 \\ 01101 \\ 10110 \\ 11011 \end{cases}$$

Tvrzení:

$(5, M, 3)$-kód C musí mít $M \leq 4$ a C_3 je jediný $(5, 4, 3)$-kód až na ekvivalenci.

Důkaz:
Předpokládejme, že slovo $\mathbf{0} = 00000$ patří kódu C.
Pak C nemůže obsahovat žádná slova s jednou 1, nebo dvěma 1, protože $d = 3$.
C může obsahovat nejvýš jedno slovo se čtyřmi nebo pěti 1. Dvě slova by se lišila na nejvýše dvou pozicích.
C musí obsahovat alespoň dvě slova s třemi 1, protože $M \geq 4$.

$$\begin{matrix} 00000 \\ 11100 \\ 00111 \end{matrix}$$

Čtvrté slovo pak zřejmě musí být:

$$11011$$

$$C_3 = \begin{cases} 00000 \\ 01101 \\ 10110 \\ 11011 \end{cases}$$

Tvrzení:

$(5, M, 3)$-kód C musí mít $M \leq 4$ a C_3 je jediný $(5, 4, 3)$-kód až na ekvivalenci.

Důkaz:
Předpokládejme, že slovo $\mathbf{0} = 00000$ patří kódu C.
Pak C nemůže obsahovat žádná slova s jednou 1, nebo dvěma 1, protože $d = 3$.
C může obsahovat nejvýš jedno slovo se čtyřmi nebo pěti 1. Dvě slova by se lišila na nejvýše dvou pozicích.
C musí obsahovat alespoň dvě slova s třemi 1, protože $M \geq 4$.

$$\begin{matrix} 00000 \\ 11100 \\ 00111 \end{matrix}$$

Čtvrté slovo pak zřejmě musí být:

$$11011$$

$$C_3 = \begin{cases} 00000 \\ 01101 \\ 10110 \\ 11011 \end{cases}$$

Tvrzení:

$(5, M, 3)$-kód C musí mít $M \leq 4$ a C_3 je jediný $(5, 4, 3)$-kód až na ekvivalenci.

Důkaz:
Předpokládejme, že slovo $\mathbf{0} = 00000$ patří kódu C.
Pak C nemůže obsahovat žádná slova s jednou 1, nebo dvěma 1, protože $d = 3$.
C může obsahovat nejvýš jedno slovo se čtyřmi nebo pěti 1. Dvě slova by se lišila na nejvýše dvou pozicích.
C musí obsahovat alespoň dvě slova s třemi 1, protože $M \geq 4$.

$$\begin{matrix} 00000 \\ 11100 \\ 00111 \end{matrix}$$

Čtvrté slovo pak zřejmě musí být:

$$11011$$

$$C_3 = \begin{cases} 00000 \\ 01101 \\ 10110 \\ 11011 \end{cases}$$

Tvrzení:

$(5, M, 3)$-kód C musí mít $M \leq 4$ a C_3 je jediný $(5, 4, 3)$-kód až na ekvivalenci.

Důkaz:
Předpokládejme, že slovo $\mathbf{0} = 00000$ patří kódu C.
Pak C nemůže obsahovat žádná slova s jednou 1, nebo dvěma 1, protože $d = 3$.
C může obsahovat nejvýš jedno slovo se čtyřmi nebo pěti 1. Dvě slova by se lišila na nejvýše dvou pozicích.
C musí obsahovat alespoň dvě slova s třemi 1, protože $M \geq 4$.

$$\begin{matrix} 00000 \\ 11100 \\ 00111 \end{matrix}$$

Čtvrté slovo pak zřejmě musí být:

$$11011$$

Hammingův horní odhad počtu slov

Nejznámnější horní odhad pro $\max M_q(n,d)$ je dán následující nerovností.

Sféra

Pro kódové slovo $\mathbf{x} \in (F_q)^n$ a celé číslo $t \geq 0$, **sférou** $S(\mathbf{x},t)$ o poloměru t a centrem $\mathbf{x}$ rozumíme množinu slov $\{\mathbf{y} \in (F_q)^n : d(\mathbf{x},\mathbf{y}) \leq t\}$.

Hammingův horní odhad

Pro q-ární $(n, M, 2t+1)$-kód platí

$$M\left\{\binom{n}{0} + \binom{n}{1}(q-1) + \ldots + \binom{n}{t}(q-1)^t\right\} \leq q^n.$$

Poznámka:
Suma $\left\{\binom{n}{0} + \binom{n}{1}(q-1) + \cdots + \binom{n}{t}(q-1)^t\right\}$ dává počet slov v množině $(F_q)^n$, která jsou obsažena ve sféře o poloměru t.

Kód, který počtem slov dosahuje Hammingova odhadu se nazývá **perfektní**.

Co je lineární kód?

Lineární kód

Abecedou kódu je konečné těleso $F_q = GF(q)$ a množinou všech slov je vektorový prostor $(F_q)^n = V(n, q)$ nad tělesem $GF(q)$.
Kód C jehož množina slov je podprostorem dimenze k v prostoru $V(n, q)$ se nazývá **lineární kód** a značí se $[n, k]$-kód, nebo $[n, k, d]$-kód.

Podmnožina C vektorového prostoru $V(n, q)$ je lineárním kódem jestliže platí:

(i) $\mathbf{x} + \mathbf{y} \in C$, pro všechna $\mathbf{x}, \mathbf{y}$ z C

(ii) $\alpha\mathbf{x} \in C$, pro každé $\alpha \in GF(q)$ a $\mathbf{x} \in C$

Výhody lineárního kódu:

- Lineární $[n, k]$-kód stačí zadat generující matici řádu $k \times n$ jejichž k řádků je tvořeno bází kódu.
- Pro lineární kód C platí $d(C) = w(C)$, kde $w(C)$ je minimální váha kódu. (obecný kód – $\binom{M}{2}$ porovnání vzdál., lineární kód – výpočet $M - 1$ vah)
- Lineární kódy umožňují snadné postupy kódování a dekódování.

Co je lineární kód?

Lineární kód

Abecedou kódu je konečné těleso $F_q = GF(q)$ a množinou všech slov je vektorový prostor $(F_q)^n = V(n, q)$ nad tělesem $GF(q)$.
Kód C jehož množina slov je podprostorem dimenze k v prostoru $V(n, q)$ se nazývá **lineární kód** a značí se $[n, k]$-kód, nebo $[n, k, d]$-kód.

Podmnožina C vektorového prostoru $V(n, q)$ je lineárním kódem jestliže platí:

(i) $\mathbf{x} + \mathbf{y} \in C$, pro všechna $\mathbf{x}, \mathbf{y}$ z C

(ii) $\alpha\mathbf{x} \in C$, pro každé $\alpha \in GF(q)$ a $\mathbf{x} \in C$

Výhody lineárního kódu:

- Lineární $[n, k]$-kód stačí zadat generující matici řádu $k \times n$ jejichž k řádků je tvořeno bází kódu.
- Pro lineární kód C platí $d(C) = w(C)$, kde $w(C)$ je minimální váha kódu. (obecný kód – $\binom{M}{2}$ porovnání vzdál., lineární kód – výpočet $M - 1$ vah)
- Lineární kódy umožňují snadné postupy kódování a dekódování.

Co je lineární kód?

Lineární kód

Abecedou kódu je konečné těleso $F_q = GF(q)$ a množinou všech slov je vektorový prostor $(F_q)^n = V(n, q)$ nad tělesem $GF(q)$.
Kód C jehož množina slov je podprostorem dimenze k v prostoru $V(n, q)$ se nazývá **lineární kód** a značí se $[n, k]$-kód, nebo $[n, k, d]$-kód.

Podmnožina C vektorového prostoru $V(n, q)$ je lineárním kódem jestliže platí:

(i) $\mathbf{x} + \mathbf{y} \in C$, pro všechna $\mathbf{x}, \mathbf{y}$ z C

(ii) $\alpha\mathbf{x} \in C$, pro každé $\alpha \in GF(q)$ a $\mathbf{x} \in C$

Výhody lineárního kódu:

- Lineární $[n, k]$-kód stačí zadat generující matici řádu $k \times n$ jejichž k řádků je tvořeno bází kódu.
- Pro lineární kód C platí $d(C) = w(C)$, kde $w(C)$ je minimální váha kódu. (obecný kód – $\binom{M}{2}$ porovnání vzdál., lineární kód – výpočet $M - 1$ vah)
- Lineární kódy umožňují snadné postupy kódování a dekódování.

Co je lineární kód?

Lineární kód

Abecedou kódu je konečné těleso $F_q = GF(q)$ a množinou všech slov je vektorový prostor $(F_q)^n = V(n, q)$ nad tělesem $GF(q)$.
Kód C jehož množina slov je podprostorem dimenze k v prostoru $V(n, q)$ se nazývá **lineární kód** a značí se $[n, k]$-kód, nebo $[n, k, d]$-kód.

Podmnožina C vektorového prostoru $V(n, q)$ je lineárním kódem jestliže platí:

(i) $\mathbf{x} + \mathbf{y} \in C$, pro všechna $\mathbf{x}, \mathbf{y}$ z C

(ii) $\alpha\mathbf{x} \in C$, pro každé $\alpha \in GF(q)$ a $\mathbf{x} \in C$

Výhody lineárního kódu:

- Lineární $[n, k]$-kód stačí zadat generující matici řádu $k \times n$ jejichž k řádků je tvořeno bází kódu.
- Pro lineární kód C platí $d(C) = w(C)$, kde $w(C)$ je minimální váha kódu. (obecný kód – $\binom{M}{2}$ porovnání vzdál., lineární kód – výpočet $M - 1$ vah)
- Lineární kódy umožňují snadné postupy kódování a dekódování.

Co je lineární kód?

Lineární kód

Abecedou kódu je konečné těleso $F_q = GF(q)$ a množinou všech slov je vektorový prostor $(F_q)^n = V(n, q)$ nad tělesem $GF(q)$.
Kód C jehož množina slov je podprostorem dimenze k v prostoru $V(n, q)$ se nazývá **lineární kód** a značí se $[n, k]$-kód, nebo $[n, k, d]$-kód.

Podmnožina C vektorového prostoru $V(n, q)$ je lineárním kódem jestliže platí:

(i) $\mathbf{x} + \mathbf{y} \in C$, pro všechna $\mathbf{x}, \mathbf{y}$ z C

(ii) $\alpha\mathbf{x} \in C$, pro každé $\alpha \in GF(q)$ a $\mathbf{x} \in C$

Výhody lineárního kódu:

- Lineární $[n, k]$-kód stačí zadat generující matici řádu $k \times n$ jejichž k řádků je tvořeno bází kódu.
- Pro lineární kód C platí $d(C) = w(C)$, kde $w(C)$ je minimální váha kódu. (obecný kód – $\binom{M}{2}$ porovnání vzdál., lineární kód – výpočet $M - 1$ vah)
- Lineární kódy umožňují snadné postupy kódování a dekódování.

Co je lineární kód?

Lineární kód

Abecedou kódu je konečné těleso $F_q = GF(q)$ a množinou všech slov je vektorový prostor $(F_q)^n = V(n, q)$ nad tělesem $GF(q)$.
Kód C jehož množina slov je podprostorem dimenze k v prostoru $V(n, q)$ se nazývá **lineární kód** a značí se $[n, k]$-kód, nebo $[n, k, d]$-kód.

Podmnožina C vektorového prostoru $V(n, q)$ je lineárním kódem jestliže platí:

(i) $\mathbf{x} + \mathbf{y} \in C$, pro všechna $\mathbf{x}, \mathbf{y}$ z C

(ii) $\alpha\mathbf{x} \in C$, pro každé $\alpha \in GF(q)$ a $\mathbf{x} \in C$

Výhody lineárního kódu:

- Lineární $[n, k]$-kód stačí zadat generující matici řádu $k \times n$ jejichž k řádků je tvořeno bází kódu.
- Pro lineární kód C platí $d(C) = w(C)$, kde $w(C)$ je minimální váha kódu. (obecný kód – $\binom{M}{2}$ porovnání vzdál., lineární kód – výpočet $M - 1$ vah)
- Lineární kódy umožňují snadné postupy kódování a dekódování.

Příklady lineárních kódů

- Binární lineární $[5, 2, 3]$-kód $\qquad C_3 = \{00000, 01101, 10110, 11011\}$

Generující matice $\mathbf{G} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}$, Kontrolní matice $\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$

- Hammingův ternární $(3, 3)$-kód je lineární $[13, 10, 3]$-kód

Kontrolní matice $H_4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}$

$M = q^{n-r} = q^k = 3^{10} = 59\,049$ slov

- Reed-Solomonův kód RS-$[255, 223]$, $(n = 255, k = 223, s = 8)$ je současně lineární $[255, 223, 33]$-kód, kde $M = 256^{223}$.

Příklady lineárních kódů

- Binární lineární $[5, 2, 3]$-kód $\quad C_3 = \{00000, 01101, 10110, 11011\}$

Generující matice $\mathbf{G} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}$, Kontrolní matice $\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$

- Hammingův ternární $(3, 3)$-kód je lineární $[13, 10, 3]$-kód

Kontrolní matice $H_4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}$

$M = q^{n-r} = q^k = 3^{10} = 59\,049$ slov

- Reed-Solomonův kód RS-$[255, 223]$, $(n = 255, k = 223, s = 8)$ je současně lineární $[255, 223, 33]$-kód, kde $M = 256^{223}$.

Příklady lineárních kódů

- Binární lineární $[5, 2, 3]$-kód $\qquad C_3 = \{00000, 01101, 10110, 11011\}$

Generující matice $\mathbf{G} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}$, Kontrolní matice $\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$

- Hammingův ternární $(3, 3)$-kód je lineární $[13, 10, 3]$-kód

Kontrolní matice $H_4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}$

$M = q^{n-r} = q^k = 3^{10} = 59\,049$ slov

- Reed-Solomonův kód RS-$[255, 223]$, $(n = 255, k = 223, s = 8)$ je současně lineární $[255, 223, 33]$-kód, kde $M = 256^{223}$.

Kódování s lineárním kódem

Binární lineární $[5, 2, 3]$-kód $\quad C_3 = \{00000, 01101, 10110, 11011\}$

Generující matice $\mathbf{G} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}$, Kontrolní matice $\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$

Kódování - kód C_3

Násobením vektoru zprávy $\mathbf{m}$ generující maticí $\mathbf{G}$ dostaneme kódový vektor/slovo $\mathbf{x}$.

zpráva $\mathbf{m}$		kódování		kódové slovo $\mathbf{x}$
00				00000
01	$\longrightarrow$	$\mathbf{mG} = \mathbf{x}$	$\longrightarrow$	01101
10				10110
11				11011

Dekódování s lineárním kódem

Binární lineární $[5, 2, 3]$-kód $C_3 = \{00000, 01101, 10110, 11011\}$

Dekódování - kód C_3

Pomocí tabulky zvané „standard array“ $(q^{n-k} \times q^k = 2^3 \times 2^2)$

Standard array

00000	**01101**	**10110**	**11011**	
00001	01100	10111	11010	1 chyba
00010	01111	10100	11001	
00100	01001	10010	11111	
01000	00101	11110	10011	
10000	11101	00110	01011	
11000	10101	01110	00011	2 chyby
10001	11100	00111	01010	

Dekódování s lineárním kódem

Binární lineární $[5, 2, 3]$-kód $\quad C_3 = \{00000, 01101, 10110, 11011\}$

Generující matice $\mathbf{G} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}$, Kontrolní matice $\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$

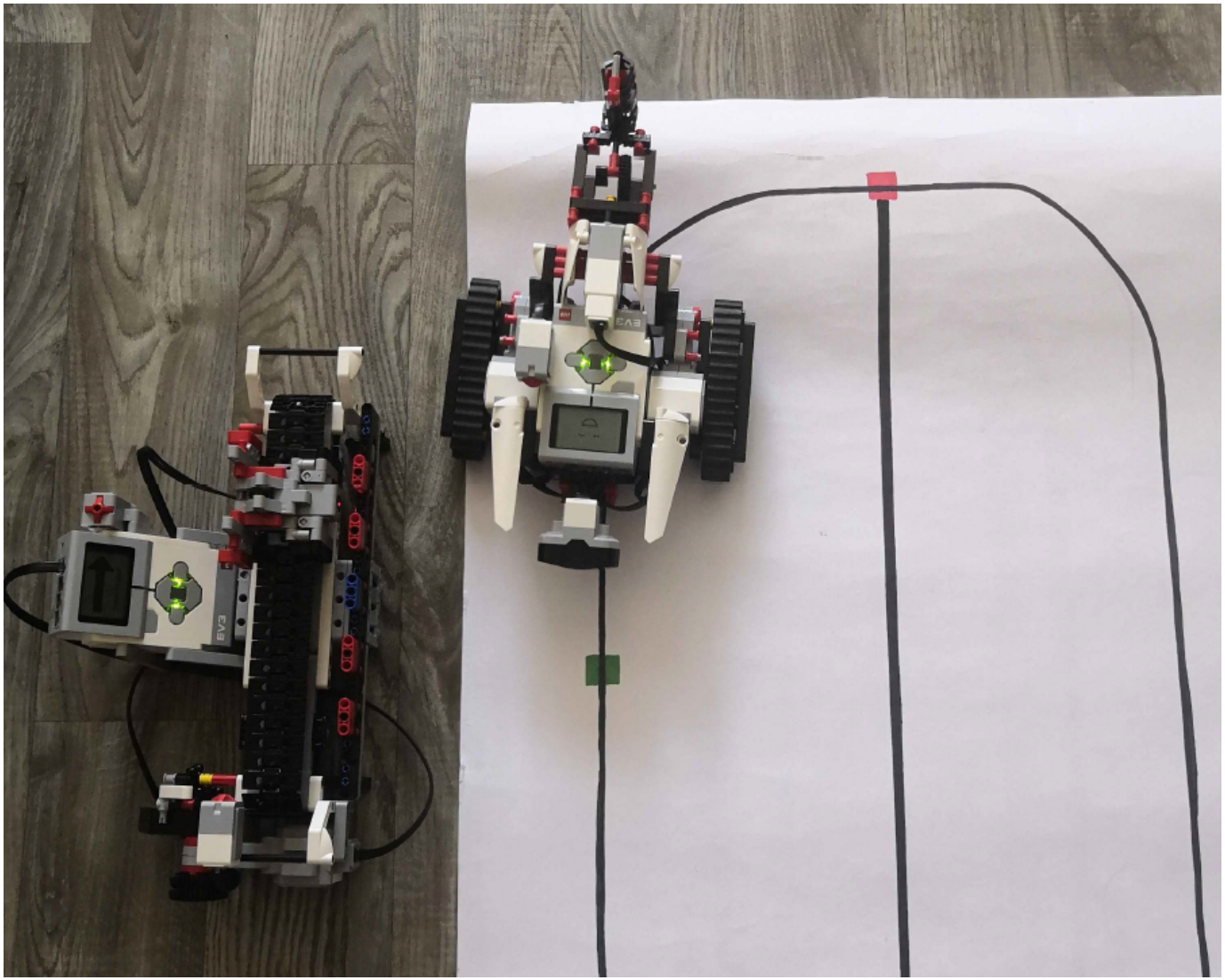
Syndromové dekódování - kód C_3

syndrom $\mathbf{s}$	reprezentant kosetu $f(\mathbf{s})$
000	00000
110	10000
011	01000
100	00100
010	00010
001	00001

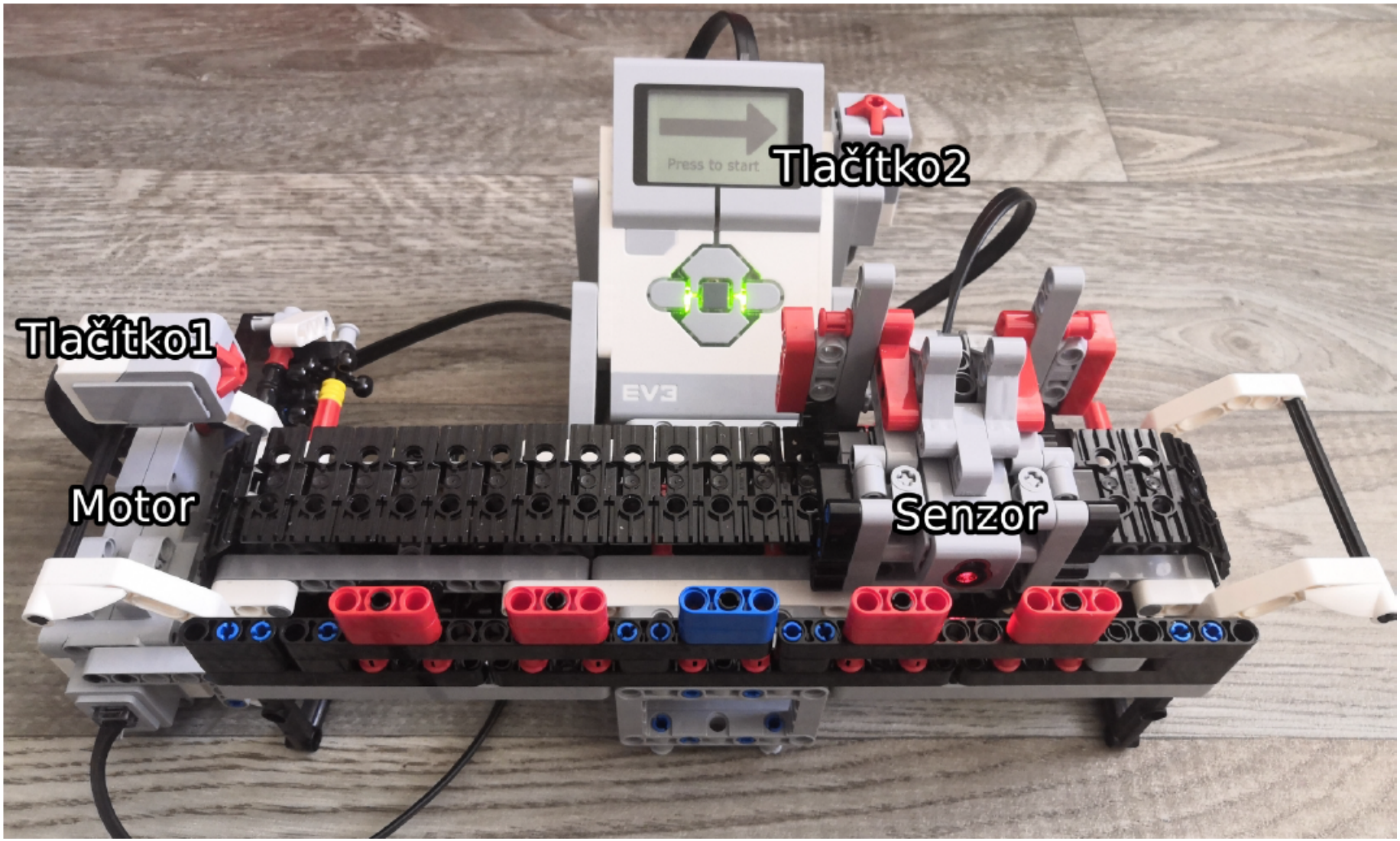
Pro přijatý vektor $\mathbf{y}$ se vypočte syndrom: $\mathbf{s}_y = \mathbf{y}\mathbf{H}^\mathbf{T}$.
Jestliže se $\mathbf{s}_y$ nachází ve sloupci se syndromy, je vektor $\mathbf{y}$ opraven na kódové slovo $\mathbf{x} = \mathbf{y} - f(\mathbf{s})$. Jinak je třeba odeslat zprávu znovu.

Příklad: Pro $\mathbf{y} = 11111$ je $\mathbf{s}_y = 010$ a vektor $\mathbf{y}$ je opraven na vektor $\mathbf{x} = 11111 - 00010 = 11101$.

LEGO robot a ukázka kódování



LEGO robot a ukázka kódování



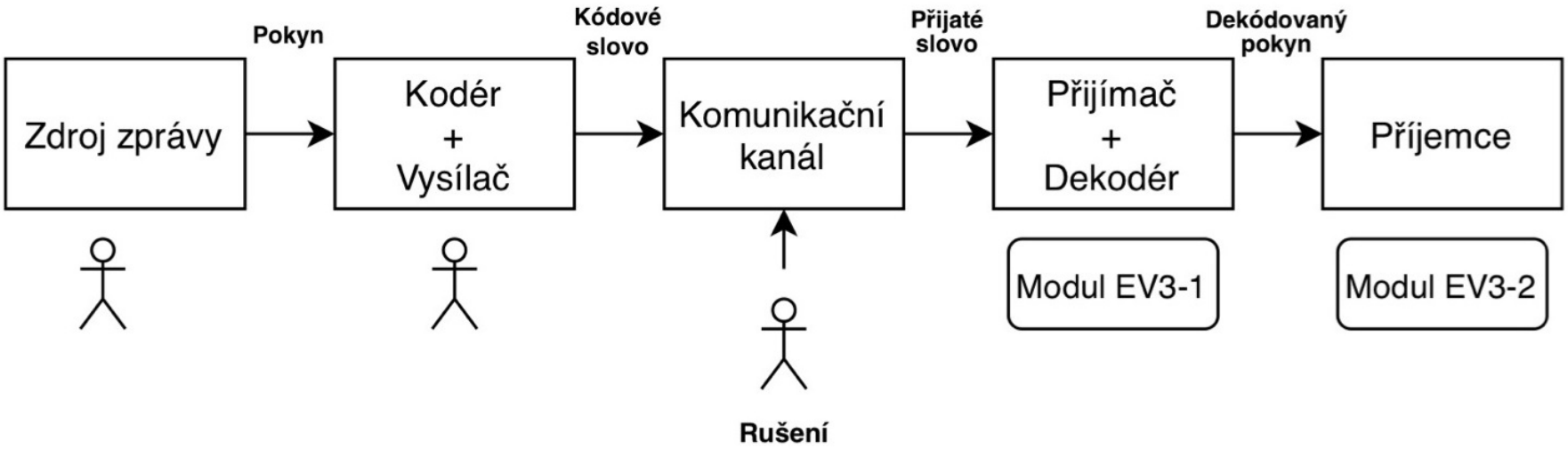
Kód použitý pro robota

Binární lineární $[5, 2, 3]$-kód $C_3 = \{00000, 01101, 10110, 11011\}$

- minimální vzdálenost: $d = 3$ (opraví 1 chybu)
- délka pokynu: $k = 2$
- počet pokynů: $M = 4$

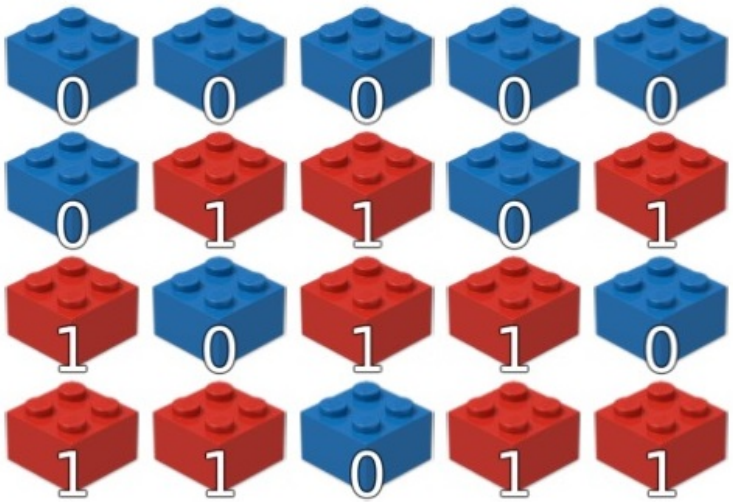
Nejkratší možná délka kódového slova: $n = 5$

Schema experimentu



Kódování pokynů pro robota

Seznam pokynů



- Změna směru
- Přechod na vnější dráhu
- Přechod na vnitřní dráhu
- Střelba

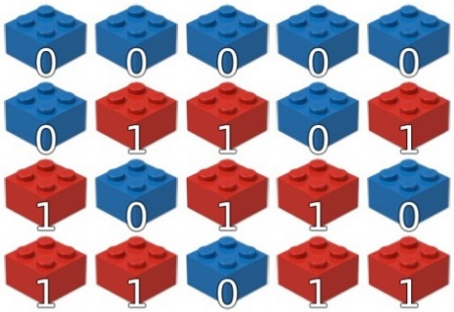
Dekódování pokynů pro robota

Standard array

00000	**01101**	**10110**	**11011**	
00001	01100	10111	11010	
00010	01111	10100	11001	
00100	01001	10010	11111	1 chyba
01000	00101	11110	10011	
10000	11101	00110	01011	
11000	10101	01110	00011	
10001	11100	00111	01010	2 chyby

Škomam Cup – otázka

(i) Jaký pokyn (kódové slovo) dostane robot po přijetí zprávy 10100 se zapnutou korekcí chyb?



- Změna směru
- Přechod na vnější dráhu
- Přechod na vnitřní dráhu
- Střelba

00000	**01101**	**10110**	**11011**
00001	01100	10111	11010
00010	01111	10100	11001
00100	01001	10010	11111
01000	00101	11110	10011
10000	11101	00110	01011
11000	10101	01110	00011
10001	11100	00111	01010

(ii) Kolik kódových slov M by měl mít ternární ($q = 3$) $(7, M, 3)$-kód, aby byl perfektní? (Nápověda: Použijte Hammingův horní odhad.)

Hammingův horní odhad

Pro q-ární $(n, M, 2t + 1)$-kód platí

$$M \left\{ \binom{n}{0} + \binom{n}{1}(q-1) + \cdots + \binom{n}{t}(q-1)^t \right\} \leq q^n.$$