

# Teorie kódování aneb jak zhustit informaci

Jan Paseka

Masarykova Univerzita Brno

14. února 2023

# Cíl přednášky

V této přednášce se pokusíme o stručný úvod do historie teorie kódování včetně teorie informace a popíšeme metody teorie kódování.

## Úvod

*Teorie kódování* je interdisciplinární teorie, která v sobě spojuje metody a postupy informatiky, matematiky a spojovací techniky.

Úlohou teorie kódování je tvorba postupů a metod, které nám zajistí bezpečný přenos zpráv komunikačním systémem.

# Teorie kódování II

**Jak postupujeme?**

## **Jak postupujeme?**

Z důvodů technické realizovatelnosti se zprávy převedou nejprve do řady znaků nad nějakou konečnou abecedou (nejlépe nad konečným tělesem).

## Jak postupujeme?

Z důvodů technické realizovatelnosti se zprávy převedou nejprve do řady znaků nad nějakou konečnou abecedou (nejlépe nad konečným tělesem).

Tato řada znaků se pak rozloží do bloků pokud možno stejné délky  $k$ . Kódovací zařízení nám pak utvoří z každého bloku délky  $k$  blok délky  $n$ , kde  $n \geq k$ .

## Jak postupujeme?

Z důvodů technické realizovatelnosti se zprávy převedou nejprve do řady znaků nad nějakou konečnou abecedou (nejlépe nad konečným tělesem).

Tato řada znaků se pak rozloží do bloků pokud možno stejné délky  $k$ . Kódovací zařízení nám pak utvoří z každého bloku délky  $k$  blok délky  $n$ , kde  $n \geq k$ .

Redundance získaná v případě kdy  $n > k$  slouží později k rozpoznání a případné opravě pokud možno co nejvíce přenosových chyb.

## Aplikace



## Aplikace

Přenos bloků délky  $n$  pomocí spojovacího systému, které reprezentují kódované zprávy a které se jako celek označují blokové kódy délky  $n$ , si lze představit buď prostorově (přes satelit, telefonem, televizí, rádiem atd.) nebo také v čase (CD, DVD, gramodeska, magnetofonová páska atd.).

## Aplikace

Přenos bloků délky  $n$  pomocí spojovacího systému, které reprezentují kódované zprávy a které se jako celek označují blokové kódy délky  $n$ , si lze představit buď prostorově (přes satelit, telefonem, televizí, rádiem atd.) nebo také v čase (CD, DVD, gramodeska, magnetofonová páska atd.).

Podíl  $k/n$  se nazývá míra informace blokového kódu a reprezentuje množství energie potřebné k přenosu kódovaných zpráv.

## Chyby při přenosu

## Chyby při přenosu

V rušeném spojovém kanálu se mohou při přenosu kódovaných zpráv vyskytnout chyby dvojího typu. Nejprve je myslitelné, že některé z vysílaných zpráv nedojdou vůbec k příjemci nebo že je příjemce obdrží neúplné.

## Chyby při přenosu

V rušeném spojovém kanálu se mohou při přenosu kódovaných zpráv vyskytnout chyby dvojího typu. Nejprve je myslitelné, že některé z vysílaných zpráv nedojdou vůbec k příjemci nebo že je příjemce obdrží neúplné.

Druhou možností je, že se mohou vyskytnout rovněž přenosové chyby, tj. vyslaný znak 0 se např. přijme jako 1; v teorii kódování se zabýváme zejména druhým případem.

## Chyby při přenosu

V rušeném spojovém kanálu se mohou při přenosu kódovaných zpráv vyskytnout chyby dvojího typu. Nejprve je myslitelné, že některé z vysílaných zpráv nedojdou vůbec k příjemci nebo že je příjemce obdrží neúplné.

Druhou možností je, že se mohou vyskytnout rovněž přenosové chyby, tj. vyslaný znak 0 se např. přijme jako 1; v teorii kódování se zabýváme zejména druhým případem.

## Oprava přenosových chyb

## Oprava přenosových chyb

Pro opravu eventuálně se vyskytujících se přenosových chyb jsou rozhodující dvě veličiny:



## Oprava přenosových chyb

Pro opravu eventuálně se vyskytujících se přenosových chyb jsou rozhodující dvě veličiny:

- ▶ míra opravitelnosti chyb, která nám udává v každé kódované zprávě podíl opravitelných chyb, a

## Oprava přenosových chyb

Pro opravu eventuálně se vyskytujících se přenosových chyb jsou rozhodující dvě veličiny:

- ▶ míra opravitelnosti chyb, která nám udává v každé kódované zprávě podíl opravitelných chyb, a
- ▶ komplexita dekóderu, který má za úlohu pro přijatou kódovanou zprávu zjistit vyslanou zprávu.

## Oprava přenosových chyb

Pro opravu eventuálně se vyskytujících se přenosových chyb jsou rozhodující dvě veličiny:

- ▶ míra opravitelnosti chyb, která nám udává v každé kódované zprávě podíl opravitelných chyb, a
- ▶ komplexita dekóderu, který má za úlohu pro přijatou kódovanou zprávu zjistit vyslanou zprávu.

Hlavním cílem teorie kódování je tvorba kódu s pokud možno co největší mírou informace a s co možná největší mírou opravitelnosti chyb při současně co možná nejmenší komplexitě dekóderu.

# Teorie kódování VI

## Teorie versus praxe

# Teorie kódování VI

## Teorie versus praxe

Shannonova věta o kapacitě kanálu nám zaručuje existenci blokových kódů s mírou informace libovolně blízce pod kapacitou kanálu, tzn. s mírou informace, která je tak vysoká jak nám to používaný kanál vůbec dovolí a s libovolně velkou mírou opravitelnosti chyb. Nekonstruktivní charakter této skutečnosti byl zrodem teorie kódování.

## Teorie versus praxe

Shannonova věta o kapacitě kanálu nám zaručuje existenci blokových kódů s mírou informace libovolně blízce pod kapacitou kanálu, tzn. s mírou informace, která je tak vysoká jak nám to používaný kanál vůbec dovolí a s libovolně velkou mírou opravitelnosti chyb. Nekonstruktivní charakter této skutečnosti byl zrodem teorie kódování.

V mnoha případech je však časová náročnost pro dekódování kódu tak velká, že neúplné využití kapacity kanálu má mnohem menší důležitost než příliš komplikovaný dekódovací postup. Z tohoto důvodu se v teorii kódování zkoumají zejména kódy s relativně jednoduchým realizovatelným dekódovacím algoritmem.

## Dodatečná struktura

## **Dodatečná struktura**

Pro určení vlastností opravujících se chyb daného kódu se ukázala důležitá dodatečná znalost jeho struktury. Proto se v teorii kódování zkoumají blokové kódy opatřené dodatečnou algebraickou strukturou, u kterých lze doufat, že budou mít v praxi použitelné teoretické vlastnosti.



## **Dodatečná struktura**

Pro určení vlastností opravujících se chyb daného kódu se ukázala důležitá dodatečná znalost jeho struktury. Proto se v teorii kódování zkoumají blokové kódy opatřené dodatečnou algebraickou strukturou, u kterých lze doufat, že budou mít v praxi použitelné teoretické vlastnosti.

Lineární kódy reprezentují jistou třídu blokových kódů a jsou opatřeny dodatečnou algebraickou strukturou – strukturou vektorového prostoru.

# Teorie kódování VIII

## Lineární kódy

# Teorie kódování VIII

## Lineární kódy

Lineární kód nad konečným tělesem  $K$  je reprezentován jako  $k$ -rozměrný podprostor  $n$ -rozměrného vektorového prostoru nad  $K$ .

# Teorie kódování VIII

## Lineární kódy

Lineární kód nad konečným tělesem  $K$  je reprezentován jako  $k$ -rozměrný podprostor  $n$ -rozměrného vektorového prostoru nad  $K$ .

Strukturu lineárních kódů lze pak analyzovat prostředky a metodami lineární algebry.

# Teorie kódování VIII

## Lineární kódy

Lineární kód nad konečným tělesem  $K$  je reprezentován jako  $k$ -rozměrný podprostor  $n$ -rozměrného vektorového prostoru nad  $K$ .

Strukturu lineárních kódů lze pak analyzovat prostředky a metodami lineární algebry.

K nejznámějším příkladům praktického použití lineárních kódů patří

- ▶ binární Reed-Mullerovy kódy – vesmírná sonda Mariner použila binární Reed-Mullerův kód prvního řádu délky 32 pro přenos datového materiálu fotodokumentace planety Mars,

# Teorie kódování VIII

## Lineární kódy

Lineární kód nad konečným tělesem  $K$  je reprezentován jako  $k$ -rozměrný podprostor  $n$ -rozměrného vektorového prostoru nad  $K$ .

Strukturu lineárních kódů lze pak analyzovat prostředky a metodami lineární algebry.

K nejznámějším příkladům praktického použití lineárních kódů patří

- ▶ binární Reed-Mullerovy kódy – vesmírná sonda Mariner použila binární Reed-Mullerův kód prvního řádu délky 32 pro přenos datového materiálu fotodokumentace planety Mars,
- ▶ Reed-Solomonovy kódy – např. se používají pro ukládání opticky kódovaných zvukových signálů na CD dva lineární kódy, které byly odvozeny zkrácením Reed-Solomonova kódu délky 255 nad tělesem  $GF(2^8)$ .

# Krátká historie I



# Krátká historie I



Algebraická a  
kombinatorická teorie  
kódování 1948 –



# Krátká historie I



Algebraická a  
kombinatorická teorie  
kódování 1948 –

# Krátká historie I



Algebraická a  
kombinatorická teorie  
kódování 1948 –



Claude E. Shannon  
(1916–2001)  
A mathematical theory  
of communication,  
Bell Systems Tech.  
Journal, 27, pp.  
623–656, October  
1948.

# Krátká historie I



Algebraická a  
kombinatorická teorie  
kódování 1948 –



Shannonova  
věta o  
kapacitě  
kanálu

Claude E. Shannon  
(1916–2001)  
A mathematical theory  
of communication,  
Bell Systems Tech.  
Journal, 27, pp.  
623–656, October  
1948.

# Krátká historie I



Algebraická a  
kombinatorická teorie  
kódování 1948 –



Shannonova  
věta o  
kapacitě  
kanálu

Claude E. Shannon  
(1916–2001)  
A mathematical theory  
of communication,  
Bell Systems Tech.  
Journal, 27, pp.  
623–656, October  
1948.

Jak ale najdeme kódy  
ze Shannonovy věty?

# Krátká historie I



Algebraická a  
kombinatorická teorie  
kódování 1948 –



Shannonova  
věta o  
kapacitě  
kanálu

Odpovědí dneška je nová, pravděpodobnostní  
teorie kódování 1994 –

Claude E. Shannon  
(1916–2001)  
A mathematical theory  
of communication,  
Bell Systems Tech.  
Journal, 27, pp.  
623–656, October  
1948.  
  
Jak ale najdeme kódy  
ze Shannonovy věty?

## Krátká historie II - Vyřešení Shannonova problému



# Krátká historie II - Vyřešení Shannonova problému



**Turbokódy a LDPC kódy:**

## Krátká historie II - Vyřešení Shannonova problému



### **Turbokódy a LDPC kódy:**

Jedná se o kódy definované na grafech s iterativními dekódovacími algoritmy!



## Krátká historie II - Vyřešení Shannonova problému



### **Turbokódy a LDPC kódy:**

Jedná se o kódy definované na grafech s iterativními dekódovacími algoritmy!

Tyto kódy jsou dostatečně náhodné, aby se opravdu hodně přiblížily kapacitě kanálu, zároveň ale jsou dostatečně konstruktivní, aby bylo možno iterativně dekódovat v polynomiálním (lineárním) čase.

## Krátká historie III - Návrat k počátkům



## Krátká historie III - Návrat k počátkům



Ve stejné době, v roce 1947, Richard W. Hamming byl jedním z prvních uživatelů na současné poměry primitivních počítačů v Bell Laboratories.

## Krátká historie III - Návrat k počátkům



Ve stejné době, v roce 1947, Richard W. Hamming byl jedním z prvních uživatelů na současné poměry primitivních počítačů v Bell Laboratories.

Frustrován jejich praktickou nepoužitelností se zaměřil na problém jak počítač může ověřit a případně opravit své vlastní výsledky.

## Krátká historie III - Návrat k počátkům



Ve stejné době, v roce 1947, Richard W. Hamming byl jedním z prvních uživatelů na současné poměry primitivních počítačů v Bell Laboratories.

Frustrován jejich praktickou nepoužitelností se zaměřil na problém jak počítač může ověřit a případně opravit své vlastní výsledky.

Výsledkem pak byla známá kontrola parity a její zobenění známé nyní jako Hammingovo kódování.

## Krátká historie III - Návrat k počátkům



Ve stejné době, v roce 1947, Richard W. Hamming byl jedním z prvních uživatelů na současné poměry primitivních počítačů v Bell Laboratories.

Frustrován jejich praktickou nepoužitelností se zaměřil na problém jak počítač může ověřit a případně opravit své vlastní výsledky.

Výsledkem pak byla známá kontrola parity a její zobenění známé nyní jako Hammingovo kódování.

Error Detecting and Error Correcting Codes, Bell System Technical Journal, vol. 29, pp. 147-160, 1950.

## Krátká historie III - Návrat k počátkům



Ve stejné době, v roce 1947, Richard W. Hamming byl jedním z prvních uživatelů na současné poměry primitivních počítačů v Bell Laboratories.

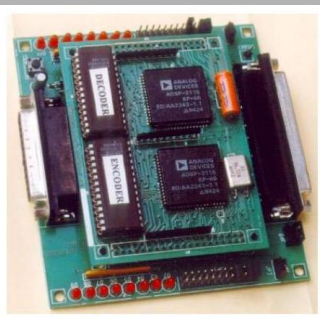
Frustrován jejich praktickou nepoužitelností se zaměřil na problém jak počítač může ověřit a případně opravit své vlastní výsledky.

Výsledkem pak byla známá kontrola parity a její zobenění známé nyní jako Hammingovo kódování.

Error Detecting and Error Correcting Codes, Bell System Technical Journal, vol. 29, pp. 147-160, 1950.

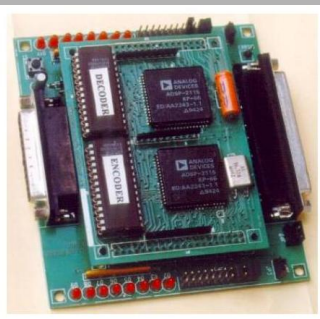
Moderní počítače by bez objevu W. Hamminga a podobných kódování jím inspirovaných nemohly existovat.

## Krátká historie IV



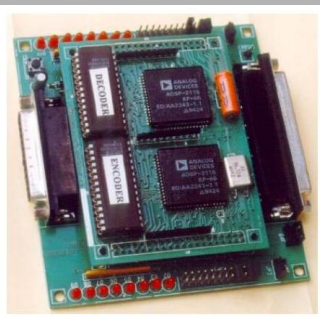


## Krátká historie IV



Milióny kódů opravující chyby jsou dekodovány každou minutu a to pomocí efektivních algoritmů implementovaných v běžných VLSI-obvodech.

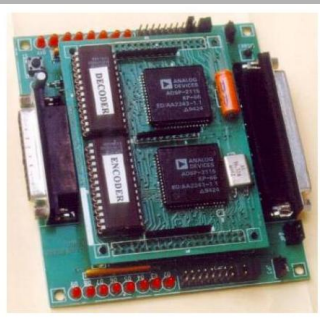
## Krátká historie IV



Miliony kódů opravující chyby jsou dekovány každou minutu a to pomocí efektivních algoritmů implementovaných v běžných VLSI-obvodech.

Alespoň 75% těchto VLSI-obvodů je dekováno pomocí Reed-Solomonových kódů.

## Krátká historie IV



Milióny kódů opravující chyby jsou dekovány každou minutu a to pomocí efektivních algoritmů implementovaných v běžných VLSI-obvodech.

Alespoň 75% těchto VLSI-obvodů je dekováno pomocí Reed-Solomonových kódů.

I.S. Reed and G. Solomon, Polynomial codes over certain finite fields, Journal Society Indust. Appl. Math. 8, pp. 300-304, June 1960.

# Teorie informace I

## Definice

*Zdroj je proud symbolů jisté konečné abecedy. Zdroj má obvykle nějaký náhodný mechanismus, který je založen na statistice situace, která je modelovaná.*

# Teorie informace I

## Definice

*Zdroj je proud symbolů jisté konečné abecedy. Zdroj má obvykle nějaký náhodný mechanismus, který je založen na statistice situace, která je modelovaná.*

Problém řešený v teorii kódování je následující:

# Teorie informace I

## Definice

*Zdroj je proud symbolů jisté konečné abecedy. Zdroj má obvykle nějaký náhodný mechanismus, který je založen na statistické situaci, která je modelovaná.*

Problém řešený v teorii kódování je následující:

Předpokládejme, že máme zdroj bez paměti  $\mathcal{S}$ , který vysílá symboly z abecedy  $W = \{w_1, \dots, w_n\}$  s pravděpodobnostmi  $\{p_1, \dots, p_n\}$ .

# Teorie informace I

## Definice

*Zdroj je proud symbolů jisté konečné abecedy. Zdroj má obvykle nějaký náhodný mechanismus, který je založen na statistice situace, která je modelovaná.*

Problém řešený v teorii kódování je následující:

Předpokládejme, že máme zdroj bez paměti  $\mathcal{S}$ , který vysílá symboly z abecedy  $W = \{w_1, \dots, w_n\}$  s pravděpodobnostmi  $\{p_1, \dots, p_n\}$ .

Prvky  $W$  budeme nazývat *zdrojová slova* a ptát se na následující otázku:

# Teorie informace I

## Definice

*Zdroj je proud symbolů jisté konečné abecedy. Zdroj má obvykle nějaký náhodný mechanismus, který je založen na statistice situace, která je modelovaná.*

Problém řešený v teorii kódování je následující:

Předpokládejme, že máme zdroj bez paměti  $\mathcal{S}$ , který vysílá symboly z abecedy  $W = \{w_1, \dots, w_n\}$  s pravděpodobnostmi  $\{p_1, \dots, p_n\}$ .

Prvky  $W$  budeme nazývat *zdrojová slova* a ptát se na následující otázku:

Je-li  $\Sigma$  abeceda  $D$  symbolů, jak můžeme zakódovat zdrojová slova  $w_i$  pomocí symbolů z  $\Sigma$ , abychom dostali co možná nejekonomičtější zakódování?



## Teorie informace II

*Kódování* neboli *kód* je zobrazení  $f$  z  $\{w_1, \dots, w_n\}$  do  $\Sigma^*$ , kde  $\Sigma^*$  označuje soubor konečných řetězců symbolů z  $\Sigma$ .

## Teorie informace II

*Kódování* neboli *kód* je zobrazení  $f$  z  $\{w_1, \dots, w_n\}$  do  $\Sigma^*$ , kde  $\Sigma^*$  označuje soubor konečných řetězců symbolů z  $\Sigma$ .

*Zpráva* je každý konečný řetězec zdrojových slov a, je-li

$$m = w_{i_1} \dots w_{i_k}$$

a je-li  $f$  kódování, pak *rozšíření  $f$*  na  $W^*$  je definováno obvyklým způsobem pomocí zřetězení

$$f(m) = f(w_{i_1}) \dots f(w_{i_k}).$$

## Teorie informace II

*Kódování* neboli *kód* je zobrazení  $f$  z  $\{w_1, \dots, w_n\}$  do  $\Sigma^*$ , kde  $\Sigma^*$  označuje soubor konečných řetězců symbolů z  $\Sigma$ .

*Zpráva* je každý konečný řetězec zdrojových slov  $a$ , je-li

$$m = w_{i_1} \dots w_{i_k}$$

a je-li  $f$  kódování, pak *rozšíření  $f$*  na  $W^*$  je definováno obvyklým způsobem pomocí zřetězení

$$f(m) = f(w_{i_1}) \dots f(w_{i_k}).$$

Kódování  $f$  je *jednoznačně dekódovatelné*, jestliže každý konečný řetězec z  $\Sigma^*$  je obraz nejvýše jedné zprávy.

## Teorie informace III

Řetězce  $f(w_i)$  se nazývají *kódová slova* a přirozená čísla  $|f(w_i)|$  jsou *slovní délky* kódování  $f$ .

## Teorie informace III

Řetězce  $f(w_i)$  se nazývají *kódová slova* a přirozená čísla  $|f(w_i)|$  jsou *slovní délky* kódování  $f$ .

*Průměrná délka*  $\langle f \rangle$  kódování  $f$  je definovaná jako

$$\langle f \rangle = \sum_{i=1}^m p_i |f(w_i)|.$$

# Teorie informace IV

Naše snaha bude určit jak efektivní takové kódování může být.

## Teorie informace IV

Naše snaha bude určit jak efektivní takové kódování může být.

Lze dokázat, že pro každý zdroj  $S$  existuje číslo, které nazýváme *entropií zdroje*  $S$  takové, že průměrná délka každého jednoznačně dekódovatelného kódování pro  $S$  musí být větší nebo rovna entropii  $S$ .

## Teorie informace IV

Naše snaha bude určit jak efektivní takové kódování může být.

Lze dokázat, že pro každý zdroj  $S$  existuje číslo, které nazýváme *entropií zdroje*  $S$  takové, že průměrná délka každého jednoznačně dekódovatelného kódování pro  $S$  musí být větší nebo rovna entropii  $S$ .

Je tedy entropie *spodní hranicí* pro každé jednoznačně dekódovatelné kódování.



## Teorie informace IV

Naše snaha bude určit jak efektivní takové kódování může být.

Lze dokázat, že pro každý zdroj  $S$  existuje číslo, které nazýváme *entropií zdroje*  $S$  takové, že průměrná délka každého jednoznačně dekódovatelného kódování pro  $S$  musí být větší nebo rovna entropii  $S$ .

Je tedy entropie *spodní hranicí* pro každé jednoznačně dekódovatelné kódování.

Účelem entropie daného zdroje je měřit množství informace ve zdroji.

# Teorie informace V

Naše představa o měření informace bude následující:

# Teorie informace V

Naše představa o měření informace bude následující:

Čím má zdrojový symbol menší pravděpodobnost výskytu, tím více informace obdržíme z výskytu tohoto symbolu a obráceně.

# Teorie informace V

Naše představa o měření informace bude následující:

Čím má zdrojový symbol menší pravděpodobnost výskytu, tím více informace obdržíme z výskytu tohoto symbolu a obráceně.

Informaci pak budeme chápat jakožto funkci pravděpodobnosti výskytu symbolu a nikoliv jako funkci tohoto symbolu.

# Teorie informace V

Naše představa o měření informace bude následující:

Čím má zdrojový symbol menší pravděpodobnost výskytu, tím více informace obdržíme z výskytu tohoto symbolu a obráceně.

Informaci pak budeme chápat jakožto funkci pravděpodobnosti výskytu symbolu a nikoliv jako funkci tohoto symbolu.

Budeme ji pak značit  $I(p)$ , kde  $0 < p \leq 1$ .

## Teorie informace VI

Předpokládejme, že  $E_1$  a  $E_2$  jsou dvě události v pravděpodobnostním prostoru  $\Omega$  spojené jistým experimentem a předpokládejme, že funkce  $I$  je naše míra informace.

## Teorie informace VI

Předpokládejme, že  $E_1$  a  $E_2$  jsou dvě události v pravděpodobnostním prostoru  $\Omega$  spojené jistým experimentem a předpokládejme, že funkce  $I$  je naše míra informace.

Mají-li  $E_1$  a  $E_2$  pravděpodobnosti  $p_1$  a  $p_2$ , pak můžeme argumentovat tím, že každá přirozená míra obsahu informace by měla splňovat

$$I(p_1 p_2) = I(p_1) + I(p_2)$$

na základě toho, že, pro dvě nezávislé realizace experimentu, informace, pro kterou výsledky těchto experimentů dopadnou jako  $E_1$  následováno  $E_2$ , by měla být součtem informací získaných provedením těchto experimentů zvlášť.

## Teorie informace VI

Předpokládejme, že  $E_1$  a  $E_2$  jsou dvě události v pravděpodobnostním prostoru  $\Omega$  spojené jistým experimentem a předpokládejme, že funkce  $I$  je naše míra informace.

Mají-li  $E_1$  a  $E_2$  pravděpodobnosti  $p_1$  a  $p_2$ , pak můžeme argumentovat tím, že každá přirozená míra obsahu informace by měla splňovat

$$I(p_1 p_2) = I(p_1) + I(p_2)$$

na základě toho, že, pro dvě nezávislé realizace experimentu, informace, pro kterou výsledky těchto experimentů dopadnou jako  $E_1$  následováno  $E_2$ , by měla být součtem informací získaných provedením těchto experimentů zvlášť.

Dále si přejeme mít naši míru nezápornou a spojitou v  $p$ , což jsou oba přirozené předpoklady.



# Teorie informace VII

## Věta

*Funkce  $I(p)$ , definovaná pro všechna  $0 < p \leq 1$ , splňuje podmínky  $I(p) \geq 0$ , pro všechna  $0 < p \leq 1$ ,  $I(p \cdot q) = I(p) + I(q)$  pro všechny  $0 < p, q \leq 1$  takové, že  $p$  a  $q$  jsou pravděpodobnosti navzájem nezávislých jevů, a podmínku spojitosti vzhledem k  $p$  právě tehdy, když je tvaru*

$$I(p) = -\lambda \log_2 p,$$

*kde  $\lambda$  je kladná konstanta.*

# Teorie informace VII

## Věta

*Funkce  $I(p)$ , definovaná pro všechna  $0 < p \leq 1$ , splňuje podmínky  $I(p) \geq 0$ , pro všechna  $0 < p \leq 1$ ,  $I(p \cdot q) = I(p) + I(q)$  pro všechny  $0 < p, q \leq 1$  takové, že  $p$  a  $q$  jsou pravděpodobnosti navzájem nezávislých jevů, a podmínku spojitosti vzhledem k  $p$  právě tehdy, když je tvaru*

$$I(p) = -\lambda \log_2 p,$$

*kde  $\lambda$  je kladná konstanta.*

## Definice

*Informaci  $I$  události  $E$  kladné pravděpodobnosti definujeme jako*

$$I(E) = -\log_2 P(E).$$

# Teorie informace VIII

Jednotkou míry informace je bit, což je zkratka pojmu binary unit.

# Teorie informace VIII

Jednotkou míry informace je bit, což je zkratka pojmu binary unit.

Spojení mezi pojmem binary unit a pojmem binary digit (rovněž se někdy zkracuje jako bit) plyne z následujícího:

## Teorie informace VIII

Jednotkou míry informace je bit, což je zkratka pojmu binary unit.

Spojení mezi pojmem binary unit a pojmem binary digit (rovněž se někdy zkracuje jako bit) plyne z následujícího:

Máme-li zdroj  $S = \{0, 1\}$  s pravděpodobnostmi  $p_0 = \frac{1}{2}$  a  $p_1 = \frac{1}{2}$ , pak informace od každého zdrojového symbolu je  $\log_2 2 = 1$ .

## Teorie informace VIII

Jednotkou míry informace je bit, což je zkratka pojmu binary unit.

Spojení mezi pojmem binary unit a pojmem binary digit (rovněž se někdy zkracuje jako bit) plyne z následujícího:

Máme-li zdroj  $S = \{0, 1\}$  s pravděpodobnostmi  $p_0 = \frac{1}{2}$  a  $p_1 = \frac{1}{2}$ , pak informace od každého zdrojového symbolu je  $\log_2 2 = 1$ .

Jinak řečeno, emituje-li zdroj náhodně jeden binary digit (bit), pak je informace získaná z jedné emise jeden binary unit (bit).

# Teorie informace IX

## Definice

*Bud'  $S$  zdroj s rozdělením pravděpodobností  $p_1, \dots, p_n$ . Entropii zdroje  $S$  definujeme jako průměrnou informaci*

$$H(S) = \sum_{k=1}^n p_k \cdot I(p_k) = - \sum_{k=1}^n p_k \cdot \log_2 p_k$$

*(suma se bere pouze přes ta  $k$ , pro která je  $p_k > 0$ ).*

# Teorie informace IX

## Definice

*Bud'  $S$  zdroj s rozdělením pravděpodobností  $p_1, \dots, p_n$ . Entropii zdroje  $S$  definujeme jako průměrnou informaci*

$$H(S) = \sum_{k=1}^n p_k \cdot I(p_k) = - \sum_{k=1}^n p_k \cdot \log_2 p_k$$

*(suma se bere pouze přes ta  $k$ , pro která je  $p_k > 0$ ).*

## **Věta o kódování bez šumu pro zdroje bez paměti**

### Věta

*Má-li zdroj bez paměti entropii  $H$ , pak každé jednoznačně dekódovatelné kódování pro tento zdroj v abecedě o  $D$  symbolech musí mít průměrnou délku alespoň  $H/\log_2 D$ . Navíc existuje takové jednoznačně dekódovatelné kódování, které má průměrnou délku slov menší nebo rovnu  $1 + H/\log_2 D$ .*



# Komunikační kanály I

Náš model komunikace – "černá skříňka", která přijímá individuální symboly na vstupu a vytváří na každý vstupní symbol nějaký výstupní symbol.

# Komunikační kanály I

Náš model komunikace – "černá skříňka", která přijímá individuální symboly na vstupu a vytváří na každý vstupní symbol nějaký výstupní symbol.

## Definice

Diskrétní kanál bez paměti *je charakterizován vstupní abecedou*  $\Sigma_1 = \{a_1, \dots, a_m\}$ , *výstupní abecedou*  $\Sigma_2 = \{b_1, \dots, b_n\}$  *a maticí*  $P$  *kanálu*

$$P = \begin{pmatrix} p_{11} & p_{12} & \dots & \dots & p_{1n-1} & p_{1n} \\ p_{21} & p_{22} & \dots & \dots & p_{2n-1} & p_{2n} \\ \vdots & \vdots & \dots & \dots & \vdots & \vdots \\ p_{m-11} & p_{m-12} & \dots & \dots & p_{m-1n-1} & p_{m-1n} \\ p_{m1} & p_{m2} & \dots & \dots & p_{mn-1} & p_{mn} \end{pmatrix},$$

zde  $p_{ij} = P(\text{symbol } b_j \text{ je obdrženo} | \text{symbol } a_i \text{ je odeslán})$ .

## Komunikační kanály II

Způsob používání kanálu je následující: každá posloupnost  $(u_1, u_2, \dots, u_N)$  symbolů ze vstupní abecedy  $\Sigma_1$  na vstupu se převede na posloupnost  $(v_1, v_2, \dots, v_N)$  téže délky symbolů z výstupní abecedy  $\Sigma_2$  na výstup tak, že

$$P(v_k = b_j | u_k = a_i) = p_{ij} \quad (1 \leq i \leq m, 1 \leq j \leq n),$$

a to nezávisle pro každé  $k$ .

## Komunikační kanály II

Způsob používání kanálu je následující: každá posloupnost  $(u_1, u_2, \dots, u_N)$  symbolů ze vstupní abecedy  $\Sigma_1$  na vstupu se převede na posloupnost  $(v_1, v_2, \dots, v_N)$  téže délky symbolů z výstupní abecedy  $\Sigma_2$  na výstup tak, že

$$P(v_k = b_j | u_k = a_i) = p_{ij} \quad (1 \leq i \leq m, 1 \leq j \leq n),$$

a to nezávisle pro každé  $k$ .

Implicitně je ve výše uvedeném obsaženo, že pro každé  $i$ ,  $1 \leq i \leq m$  platí

$$\sum_j p_{ij} = 1.$$

## Komunikační kanály II

Způsob používání kanálu je následující: každá posloupnost  $(u_1, u_2, \dots, u_N)$  symbolů ze vstupní abecedy  $\Sigma_1$  na vstupu se převede na posloupnost  $(v_1, v_2, \dots, v_N)$  téže délky symbolů z výstupní abecedy  $\Sigma_2$  na výstup tak, že

$$P(v_k = b_j | u_k = a_i) = p_{ij} \quad (1 \leq i \leq m, 1 \leq j \leq n),$$

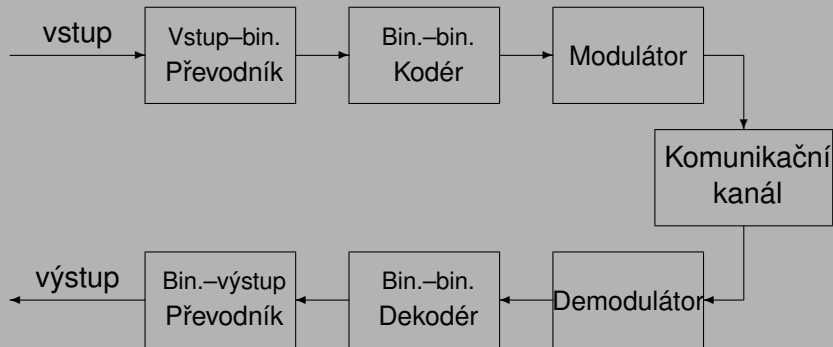
a to nezávisle pro každé  $k$ .

Implicitně je ve výše uvedeném obsaženo, že pro každé  $i$ ,  $1 \leq i \leq m$  platí

$$\sum_j p_{ij} = 1.$$

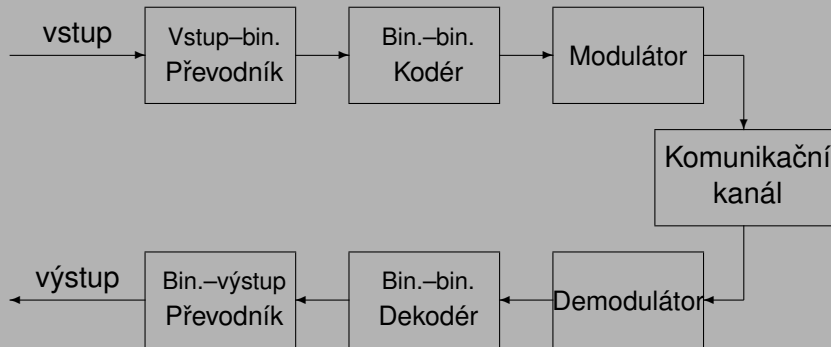
Matice  $P$  s nezápornými hodnotami taková, že součet prvků v každém řádku je roven 1, se nazývá *stochastická matice*; v teorii náhodných procesů mluvíme o matici přechodu markovského řetězce.

# Komunikační kanály III



Obrázek: Konkrétní sdělovací systém.

## Komunikační kanály III



**Obrázek:** Konkrétní sdělovací systém.

Kodéry (převodníky) převádí znaky jedné abecedy na znaky abecedy jiné. Modulátor na vstupu přijímá jednotlivé znaky a ke každému znaku vytváří proudový impuls, který vstupuje do kanálu.

# Komunikační kanály IV

## Příklad

Binární vypouštěcí kanál *má vstupní abecedu*  $\Sigma_1 = \{0, 1\}$ ,  
*výstupní abecedu*  $\Sigma_2 = \{0, 1, *\}$  *a maticí*  $P$  *kanálu*

$$P = \begin{pmatrix} 1 - \varepsilon & 0 & \varepsilon \\ 0 & 1 - \varepsilon & \varepsilon \end{pmatrix}.$$



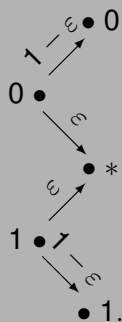
# Komunikační kanály IV

## Příklad

Binární vypouštěcí kanál má vstupní abecedu  $\Sigma_1 = \{0, 1\}$ , výstupní abecedu  $\Sigma_2 = \{0, 1, *\}$  a maticí  $P$  kanálu

$$P = \begin{pmatrix} 1 - \varepsilon & 0 & \varepsilon \\ 0 & 1 - \varepsilon & \varepsilon \end{pmatrix}.$$

Diagram odpovídající tomuto kanálu má tvar



# Komunikační kanály IV

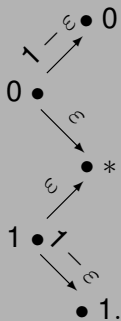
## Příklad

Binární vypouštěcí kanál má vstupní abecedu  $\Sigma_1 = \{0, 1\}$ , výstupní abecedu  $\Sigma_2 = \{0, 1, *\}$  a maticí  $P$  kanálu

$$P = \begin{pmatrix} 1 - \varepsilon & 0 & \varepsilon \\ 0 & 1 - \varepsilon & \varepsilon \end{pmatrix}.$$

*Diagram odpovídající tomuto kanálu má tvar*

*To odpovídá situaci, pro kterou má každý symbol pravděpodobnost  $\varepsilon$ , že se špatně přenese a to na \*. Ale jak 1 tak 0 nelze navzájem zaměnit.*



# Kódování a dekódovací pravidla I

## Kódování a dekódovací pravidla

Bud' dán kanál bez paměti se vstupní abecedou

$\Sigma_1 = \{a_1, \dots, a_m\}$  a výstupní abecedou  $\Sigma_2 = \{b_1, \dots, b_k\}$ .

# Kódování a dekodovací pravidla I

## Kódování a dekodovací pravidla

Bud' dán kanál bez paměti se vstupní abecedou

$\Sigma_1 = \{a_1, \dots, a_m\}$  a výstupní abecedou  $\Sigma_2 = \{b_1, \dots, b_k\}$ .

*Kód délky  $n$*  je libovolný systém  $\mathcal{C}$  různých posloupností délky  $n$  symbolů ze  $\Sigma_1$ .

# Kódování a dekodovací pravidla I

## Kódování a dekodovací pravidla

Bud' dán kanál bez paměti se vstupní abecedou

$\Sigma_1 = \{a_1, \dots, a_m\}$  a výstupní abecedou  $\Sigma_2 = \{b_1, \dots, b_k\}$ .

*Kód délky  $n$*  je libovolný systém  $\mathcal{C}$  různých posloupností délky  $n$  symbolů ze  $\Sigma_1$ .

Prvky z  $\mathcal{C}$  se nazývají *kódová slova*.

# Kódování a dekodovací pravidla I

## Kódování a dekodovací pravidla

Bud' dán kanál bez paměti se vstupní abecedou

$\Sigma_1 = \{a_1, \dots, a_m\}$  a výstupní abecedou  $\Sigma_2 = \{b_1, \dots, b_k\}$ .

*Kód délky  $n$*  je libovolný systém  $\mathcal{C}$  různých posloupností délky  $n$  symbolů ze  $\Sigma_1$ .

Prvky z  $\mathcal{C}$  se nazývají *kódová slova*.

Je-li dán kód délky  $n$  s kódovými slovy  $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_N$ ,

*dekodovací pravidlo* je libovolný rozklad množiny možných obdržených posloupností do disjunktních množin

$R_1, R_2, \dots, R_N$  se zřejmou interpretací toho, že je-li obdržená posloupnost  $\mathbf{y}$  prvkem množiny  $R_j$ , je  $\mathbf{y}$  dekodováno jako kódové slovo  $\mathbf{c}_j$ .

## Kódování a dekodovací pravidla II

Formálně vzato, předpokládáme-li, že kód  $\mathcal{C}$  neobsahuje např. symbol "?" jakožto kódové slovo, *rozhodovací (dekodovací) pravidlo* pro kód  $\mathcal{C}$  je funkce  $f : \Sigma_2^n \rightarrow \mathcal{C} \cup \{?\}$ .

## Kódování a dekodovací pravidla II

Formálně vzato, předpokládáme-li, že kód  $\mathcal{C}$  neobsahuje např. symbol "?" jakožto kódové slovo, *rozhodovací (dekodovací) pravidlo* pro kód  $\mathcal{C}$  je funkce  $f : \Sigma_2^n \rightarrow \mathcal{C} \cup \{?\}$ .  
Aplikaci dekodovacího pravidla nazýváme *dekódování*.



## Kódování a dekodovací pravidla II

Formálně vzato, předpokládáme-li, že kód  $\mathcal{C}$  neobsahuje např. symbol "?" jakožto kódové slovo, *rozhodovací (dekodovací) pravidlo* pro kód  $\mathcal{C}$  je funkce  $f : \Sigma_2^n \rightarrow \mathcal{C} \cup \{?\}$ .

Aplikaci dekodovacího pravidla nazýváme *dekódování*.

Je-li  $\mathbf{y}$  (obdržené) slovo v  $\Sigma_2^n$ , pak rozhodovací pravidlo *dekóduje*  $\mathbf{y}$  jakožto kódové slovo  $f(\mathbf{y})$  nebo v opačném případě nahlásí *dekodovací chybu*, jestliže  $f(\mathbf{y}) = ?$ .

## Kódování a dekodovací pravidla II

Formálně vzato, předpokládáme-li, že kód  $\mathcal{C}$  neobsahuje např. symbol "?" jakožto kódové slovo, *rozhodovací (dekodovací) pravidlo* pro kód  $\mathcal{C}$  je funkce  $f : \Sigma_2^n \rightarrow \mathcal{C} \cup \{?\}$ .

Aplikaci dekodovacího pravidla nazýváme *dekódování*.

Je-li  $\mathbf{y}$  (obdržené) slovo v  $\Sigma_2^n$ , pak rozhodovací pravidlo *dekóduje*  $\mathbf{y}$  jakožto kódové slovo  $f(\mathbf{y})$  nebo v opačném případě nahlásí *dekodovací chybu*, jestliže  $f(\mathbf{y}) = ?$ .

Výběr dekodovacího pravidla je podstatný k úspěchu každého komunikačního systému.

# Kódování a dekodovací pravidla III

## Hammingovo paradigma

Jsou-li  $\mathbf{x}$  a  $\mathbf{y}$  vektory z  $\mathbf{F}_q^n$ , definujme *Hammingovu vzdálenost*  $d(\mathbf{x}, \mathbf{y})$  mezi  $\mathbf{x}$  a  $\mathbf{y}$  jako počet míst, ve kterých se  $\mathbf{x}$  a  $\mathbf{y}$  liší.

# Kódování a dekodovací pravidla III

## Hammingovo paradigma

Jsou-li  $\mathbf{x}$  a  $\mathbf{y}$  vektory z  $\mathbf{F}_q^n$ , definujme *Hammingovu vzdálenost*  $d(\mathbf{x}, \mathbf{y})$  mezi  $\mathbf{x}$  a  $\mathbf{y}$  jako počet míst, ve kterých se  $\mathbf{x}$  a  $\mathbf{y}$  liší.



# Kódování a dekodovací pravidla III

## Hammingovo paradigma

Jsou-li  $\mathbf{x}$  a  $\mathbf{y}$  vektory z  $\mathbf{F}_q^n$ , definujme *Hammingovu vzdálenost*  $d(\mathbf{x}, \mathbf{y})$  mezi  $\mathbf{x}$  a  $\mathbf{y}$  jako počet míst, ve kterých se  $\mathbf{x}$  a  $\mathbf{y}$  liší. *Minimální vzdálenost kódu*  $\mathcal{C}$  je číslo

$$d = d(\mathcal{C}) = \min d(\mathbf{c}_i, \mathbf{c}_j),$$

kde je minimum bráno přes všechny navzájem různé dvojice kódových slov z  $\mathcal{C}$ .



# Kódování a dekodovací pravidla III

## Hammingovo paradigma

Jsou-li  $\mathbf{x}$  a  $\mathbf{y}$  vektory z  $\mathbf{F}_q^n$ , definujme *Hammingovu vzdálenost*  $d(\mathbf{x}, \mathbf{y})$  mezi  $\mathbf{x}$  a  $\mathbf{y}$  jako počet míst, ve kterých se  $\mathbf{x}$  a  $\mathbf{y}$  liší. *Minimální vzdálenost kódu*  $\mathcal{C}$  je číslo

$$d = d(\mathcal{C}) = \min d(\mathbf{c}_i, \mathbf{c}_j),$$

kde je minimum bráno přes všechny navzájem různé dvojice kódových slov z  $\mathcal{C}$ .

Má-li kódování minimální vzdálenost  $d$ , můžeme jej považovat za rozmístění navzájem disjunktních koulí o poloměru  $t = \lfloor (d - 1)/2 \rfloor$  v Hammingově prostoru  $\mathbf{F}_q^n$ .



# Kódování a dekodovací pravidla III

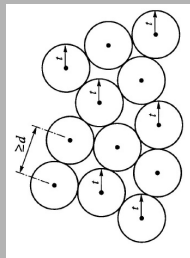
## Hammingovo paradigma

Jsou-li  $\mathbf{x}$  a  $\mathbf{y}$  vektory z  $\mathbf{F}_q^n$ , definujme *Hammingovu vzdálenost*  $d(\mathbf{x}, \mathbf{y})$  mezi  $\mathbf{x}$  a  $\mathbf{y}$  jako počet míst, ve kterých se  $\mathbf{x}$  a  $\mathbf{y}$  liší. *Minimální vzdálenost kódu*  $\mathcal{C}$  je číslo

$$d = d(\mathcal{C}) = \min d(\mathbf{c}_i, \mathbf{c}_j),$$

kde je minimum bráno přes všechny navzájem různé dvojice kódových slov z  $\mathcal{C}$ .

Má-li kódování minimální vzdálenost  $d$ , můžeme jej považovat za rozmístění navzájem disjunktních koulí o poloměru  $t = \lfloor (d - 1)/2 \rfloor$  v Hammingově prostoru  $\mathbf{F}_q^n$ .



# Kódování a dekodovací pravidla III

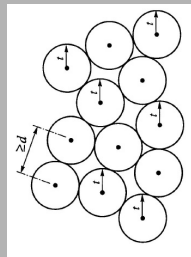
## Hammingovo paradigma

Jsou-li  $\mathbf{x}$  a  $\mathbf{y}$  vektory z  $\mathbf{F}_q^n$ , definujme *Hammingovu vzdálenost*  $d(\mathbf{x}, \mathbf{y})$  mezi  $\mathbf{x}$  a  $\mathbf{y}$  jako počet míst, ve kterých se  $\mathbf{x}$  a  $\mathbf{y}$  liší. *Minimální vzdálenost kódu*  $\mathcal{C}$  je číslo

$$d = d(\mathcal{C}) = \min d(\mathbf{c}_i, \mathbf{c}_j),$$

kde je minimum bráno přes všechny navzájem různé dvojice kódových slov z  $\mathcal{C}$ .

Má-li kódování minimální vzdálenost  $d$ , můžeme jej považovat za rozmístění navzájem disjunktních koulí o poloměru  $t = \lfloor (d - 1)/2 \rfloor$  v Hammingově prostoru  $\mathbf{F}_q^n$ .



Takovýto kód opraví až  $t$  chyb.



# Kódování a dekodovací pravidla III

## Hammingovo paradigma

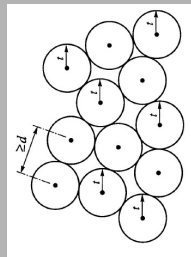
Jsou-li  $\mathbf{x}$  a  $\mathbf{y}$  vektory z  $\mathbf{F}_q^n$ , definujme *Hammingovu vzdálenost*  $d(\mathbf{x}, \mathbf{y})$  mezi  $\mathbf{x}$  a  $\mathbf{y}$  jako počet míst, ve kterých se  $\mathbf{x}$  a  $\mathbf{y}$  liší. *Minimální vzdálenost kódu*  $\mathcal{C}$  je číslo

$$d = d(\mathcal{C}) = \min d(\mathbf{c}_i, \mathbf{c}_j),$$

kde je minimum bráno přes všechny navzájem různé dvojice kódových slov z  $\mathcal{C}$ .

Má-li kódování minimální vzdálenost  $d$ , můžeme jej považovat za rozmístění navzájem disjunktních koulí o poloměru  $t = \lfloor (d - 1)/2 \rfloor$  v Hammingově prostoru  $\mathbf{F}_q^n$ .

Lze tedy pohlížet na teorii kódování jako na kombinatorickou úlohu o rozmístění koulí hustě a efektivně v metrických prostorech.



Takovýto kód opraví až  $t$  chyb.

# Kódování a dekodovací pravidla IV

## Jaké jsou nejlepší kódy?

$A_q(n, d)$  = největší počet vektorů délky  $n$  nad abecedou s  $q$  písmeny tak, že každé dva různé vektory mají vzdálenost alespoň  $d$ .

# Kódování a dekodovací pravidla IV

## Jaké jsou nejlepší kódy?

$A_q(n, d)$  = největší počet vektorů délky  $n$  nad abecedou s  $q$  písmeny tak, že každé dva různé vektory mají vzdálenost alespoň  $d$ .



# Kódování a dekodovací pravidla IV

## Jaké jsou nejlepší kódy?

$A_q(n, d)$  = největší počet vektorů délky  $n$  nad abecedou s  $q$  písmeny tak, že každé dva různé vektory mají vzdálenost alespoň  $d$ .

$S_q(n, d)$  = objem Hammingovy sféry o poloměru  $d$  ve vektorovém prostoru  $n$ -tic nad abecedou s  $q$  písmeny.



# Kódování a dekodovací pravidla IV

## Jaké jsou nejlepší kódy?

$A_q(n, d)$  = největší počet vektorů délky  $n$  nad abecedou s  $q$  písmeny tak, že každé dva různé vektory mají vzdálenost alespoň  $d$ .

$S_q(n, d)$  = objem Hammingovy sféry o poloměru  $d$  ve vektorovém prostoru  $n$ -tic nad abecedou s  $q$  písmeny.



### Věta (Gilbert-Varshamova hranice)

$$A_q(n, d) \geq \frac{q^n}{\sum_{k=0}^{d-1} \binom{n}{k} (q-1)^k} = \frac{q^n}{S_q(n, d-1)}$$

# Kódování a dekodovací pravidla IV

## Jaké jsou nejlepší kódy?

$A_q(n, d)$  = největší počet vektorů délky  $n$  nad abecedou s  $q$  písmeny tak, že každé dva různé vektory mají vzdálenost alespoň  $d$ .

$S_q(n, d)$  = objem Hammingovy sféry o poloměru  $d$  ve vektorovém prostoru  $n$ -tic nad abecedou s  $q$  písmeny.



### Věta (Gilbert-Varshamova hranice)

$$A_q(n, d) \geq \frac{q^n}{\sum_{k=0}^{d-1} \binom{n}{k} (q-1)^k} = \frac{q^n}{S_q(n, d-1)}$$

E.N. Gilbert, A comparison of signaling alphabets, Bell Systems Technical Journal, October 1952.

# Kódování a dekódovací pravidla IV

## Důkaz Gilbert-Varshamovy hranice

.

# Kódování a dekodovací pravidla IV

## Důkaz Gilbert-Varshamovy hranice

Fixujme libovolný vektor  $\mathbf{x}$  z dané množiny vektorů, přidejme jej do konstruovaného kódování a odstraňme z dané množiny Hammingovu sféru o střed  $\mathbf{x}$  a poloměru  $d - 1$ .



# Kódování a dekodovací pravidla IV

## Důkaz Gilbert-Varshamovy hranice

Fixujme libovolný vektor  $\mathbf{x}$  z dané množiny vektorů, přidejme jej do konstruovaného kódování a odstraňme z dané množiny Hammingovu sféru o střed  $\mathbf{x}$  a poloměru  $d - 1$ .

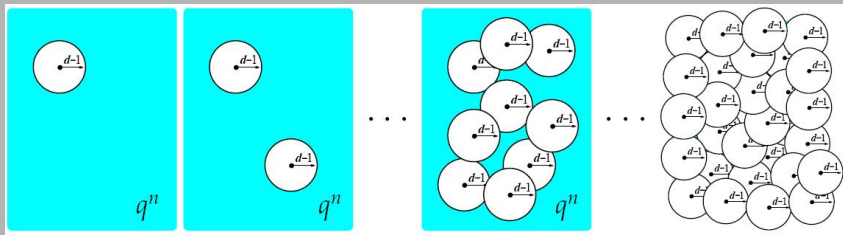
Postup opakujme.

# Kódování a dekodovací pravidla IV

## Důkaz Gilbert-Varshamovy hranice

Fixujme libovolný vektor  $\mathbf{x}$  z dané množiny vektorů, přidejme jej do konstruovaného kódování a odstraňme z dané množiny Hammingovu sféru o střed  $\mathbf{x}$  a poloměru  $d - 1$ .

Postup opakujme.

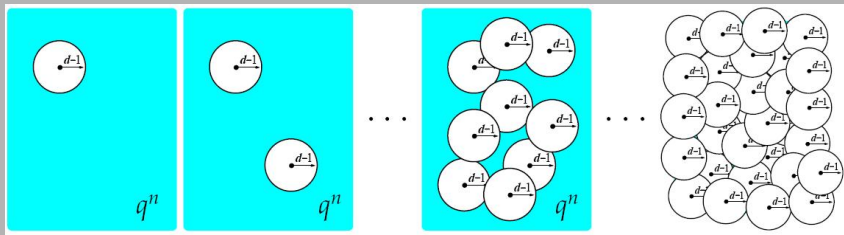


# Kódování a dekodovací pravidla IV

## Důkaz Gilbert-Varshamovy hranice

Fixujme libovolný vektor  $\mathbf{x}$  z dané množiny vektorů, přidejme jej do konstruovaného kódování a odstraňme z dané množiny Hammingovu sféru o středu  $\mathbf{x}$  a poloměru  $d - 1$ .

Postup opakujeme.



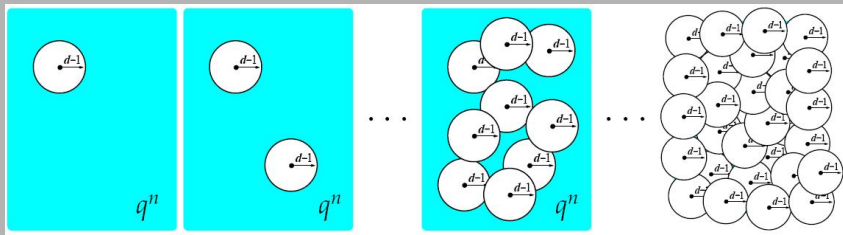
Jestliže po  $M$  krocích nic v dané množině nezůstane, nutně  $M$  sfér se středy, jež jsou kódová slova, pokrývá celý prostor  $\mathbf{F}_q^n$ .

# Kódování a dekodovací pravidla IV

## Důkaz Gilbert-Varshamovy hranice

Fixujme libovolný vektor  $\mathbf{x}$  z dané množiny vektorů, přidejme jej do konstruovaného kódování a odstraňme z dané množiny Hammingovu sféru o středě  $\mathbf{x}$  a poloměru  $d - 1$ .

Postup opakujeme.



Jestliže po  $M$  krocích nic v dané množině nezůstane, nutně  $M$  sfér se středě, jež jsou kódová slova, pokrývá celý prostor  $\mathbf{F}_q^n$ .

Nutně tedy  $M \sum_{k=0}^{d-1} \binom{n}{k} (q-1)^k \geq q^n$ .

# Kódování a dekodovací pravidla V

## Hammingova hranice a perfektní kódy

# Kódování a dekodovací pravidla V

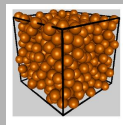
## Hammingova hranice a perfektní kódy

$$\frac{q^n}{S_q(n, 2e)} \leq A_q(n, 2e + 1) \leq \frac{q^n}{S_q(n, e)}$$

# Kódování a dekodovací pravidla V

## Hammingova hranice a perfektní kódy

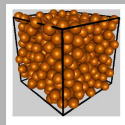
$$\frac{q^n}{S_q(n, 2e)} \leq A_q(n, 2e + 1) \leq \frac{q^n}{S_q(n, e)}$$



# Kódování a dekodovací pravidla V

## Hammingova hranice a perfektní kódy

$$\frac{q^n}{S_q(n, 2e)} \leq A_q(n, 2e + 1) \leq \frac{q^n}{S_q(n, e)}$$



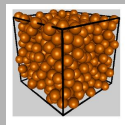
Ideální situace z ekonomického pohledu je najít kód  $\mathcal{C}$  nad  $\mathbf{F}_q^n$  tak, že pro jisté kladné  $t > 0$  jsou všechny prvky z  $\mathbf{F}_q^n$  obsaženy v disjunktivním sjednocení koulí, jejichž středy jsou navzájem různá kódová slova. Takový kód se pak nazývá *perfektní*.



# Kódování a dekodovací pravidla V

## Hammingova hranice a perfektní kódy

$$\frac{q^n}{S_q(n, 2e)} \leq A_q(n, 2e + 1) \leq \frac{q^n}{S_q(n, e)}$$



Ideální situace z ekonomického pohledu je najít kód  $\mathcal{C}$  nad  $\mathbf{F}_q^n$  tak, že pro jisté kladné  $t > 0$  jsou všechny prvky z  $\mathbf{F}_q^n$  obsaženy v disjunktním sjednocení koulí, jejichž středy jsou navzájem různá kódová slova. Takový kód se pak nazývá *perfektní*.

Příklady perfektního kódu:

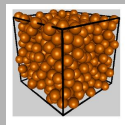
1. každý kód s právě jedním kódovým slovem,
2. každý binární kód s právě dvěma slovy lichých délek, např.  $00 \dots 0$  a  $11 \dots 1$ .

*Triviální perfektní kódy*

# Kódování a dekodovací pravidla V

## Hammingova hranice a perfektní kódy

$$\frac{q^n}{S_q(n, 2e)} \leq A_q(n, 2e + 1) \leq \frac{q^n}{S_q(n, e)}$$



Ideální situace z ekonomického pohledu je najít kód  $\mathcal{C}$  nad  $\mathbf{F}_q^n$  tak, že pro jisté kladné  $t > 0$  jsou všechny prvky z  $\mathbf{F}_q^n$  obsaženy v disjunktním sjednocení koulí, jejichž středy jsou navzájem různá kódová slova. Takový kód se pak nazývá *perfektní*.

Příklady perfektního kódu:

1. každý kód s právě jedním kódovým slovem,
2. každý binární kód s právě dvěma slovy lichých délek, např.  $00 \dots 0$  a  $11 \dots 1$ .
3.  $(n, n - m, 3)$  Hammingovy kódy pro  $n = 2^m - 1$ ,
4.  $(23, 12, 7)$  binární Golayův kód.

*Triviální perfektní kódy*

*Netriviální perfektní kódy*

## Singletonova hranice a MDS kódy

## Singletonova hranice a MDS kódy

$$A_q(n, d) \leq q^{n-d+1}$$

### Příklady MDS kódů

- ▶ Reed-Solomonovy kódy a zobecněné Reed-Solomonovy kódy

# Kódování a dekodovací pravidla VI

## Singletonova hranice a MDS kódy

Seznam všech kódových slov

$$A_q(n, d) \leq q^{n-d+1}$$

				...			} $d - 1$

## Příklady MDS kódů

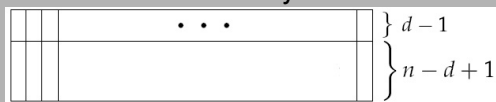
- ▶ Reed-Solomonovy kódy a zobecněné Reed-Solomonovy kódy

# Kódování a dekodovací pravidla VI

## Singletonova hranice a MDS kódy

Seznam všech kódových slov

$$A_q(n, d) \leq q^{n-d+1}$$



Kódy, pro které nastane v Singletonově hranici rovnost, se nazývají *MDS kódy* (maximum distance separable).

### Příklady MDS kódů

- ▶ Reed-Solomonovy kódy a zobecněné Reed-Solomonovy kódy

# Kódování a dekódovací pravidla VII

## Konstrukce Reed-Solomonových kódů

Popíšeme kódování pomocí kódovacího předpisu  $\mathcal{E} : \mathbf{F}_q^k \rightarrow \mathbf{F}_q^n$ .

# Kódování a dekodovací pravidla VII

## Konstrukce Reed-Solomonových kódů

Popíšeme kódování pomocí kódovacího předpisu  $\mathcal{E} : \mathbf{F}_q^k \rightarrow \mathbf{F}_q^n$ .

Zafixujme přirozená čísla  $k \leq n \leq q$  a  $n$  různých prvků

$x_1, \dots, x_n \in \mathbf{F}_q$ .



# Kódování a dekódovací pravidla VII

## Konstrukce Reed-Solomonových kódů

Popíšeme kódování pomocí kódovacího předpisu  $\mathcal{E} : \mathbf{F}_q^k \rightarrow \mathbf{F}_q^n$ .

Zafixujme přirozená čísla  $k \leq n \leq q$  a  $n$  různých prvků  $x_1, \dots, x_n \in \mathbf{F}_q$ . Pak z  $k$  informačních symbolů obdržíme  $n$  kódových slov.

# Kódování a dekodovací pravidla VII

## Konstrukce Reed-Solomonových kódů

Popíšeme kódování pomocí kódovacího předpisu  $\mathcal{E} : \mathbf{F}_q^k \rightarrow \mathbf{F}_q^n$ .  
Zafixujeme přirozená čísla  $k \leq n \leq q$  a  $n$  různých prvků  $x_1, \dots, x_n \in \mathbf{F}_q$ . Pak z  $k$  informačních symbolů obdržíme  $n$  kódových slov.

$$\begin{array}{c} u_0, u_1, \dots, u_{k-1} \\ \Downarrow \\ \underline{f}(X) = u_0 + u_1X + \dots + u_{k-1}X^{k-1} \\ \Downarrow \\ c_1 = \underline{f}(x_1), c_2 = \underline{f}(x_2), \dots, c_n = \underline{f}(x_n) \\ \Downarrow \\ (c_1, c_2, \dots, c_n) \end{array}$$

# Kódování a dekódovací pravidla VII

## Konstrukce Reed-Solomonových kódů

Popíšeme kódování pomocí kódovacího předpisu  $\mathcal{E} : \mathbf{F}_q^k \rightarrow \mathbf{F}_q^n$ .  
Zafixujeme přirozená čísla  $k \leq n \leq q$  a  $n$  různých prvků  $x_1, \dots, x_n \in \mathbf{F}_q$ . Pak z  $k$  informačních symbolů obdržíme  $n$  kódových slov.

$$\begin{array}{c} u_0, u_1, \dots, u_{k-1} \\ \Downarrow \\ f_{\underline{u}}(X) = u_0 + u_1X + \dots + u_{k-1}X^{k-1} \\ \Downarrow \\ c_1 = f_{\underline{u}}(x_1), c_2 = f_{\underline{u}}(x_2), \dots, c_n = f_{\underline{u}}(x_n) \\ \Downarrow \\ (c_1, c_2, \dots, c_n) \end{array}$$

Reed-Solomonovy kódy jsou lineární. Mají poměr  $R = k/n$  a vzdálenost  $d = n - k + 1$ , která je nejlepší možná (MDS).

# Kódování a dekodovací pravidla VIII

## **Algebraické dekodování Reed-Solomonových kódů**

## Algebraické dekódování Reed-Solomonových kódů

- ▶ Každé kódové slovo Reed-Solomonova kódu  $\mathbf{C}_q(n, k)$  sestává z nějakých  $n$  hodnot polynomu  $f(X)$ , který je stupně  $< k$ .

## Algebraické dekódování Reed-Solomonových kódů

- ▶ Každé kódové slovo Reed-Solomonova kódu  $\mathbf{C}_q(n, k)$  sestává z nějakých  $n$  hodnot polynomu  $f(X)$ , který je stupně  $< k$ . Tento polynom můžeme jednoznačně zpětně určit interpolací jeho libovolných  $k$  funkčních hodnot.

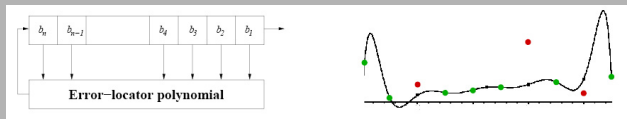
# Kódování a dekodovací pravidla VIII

## Algebraické dekodování Reed-Solomonových kódů

- ▶ Každé kódové slovo Reed-Solomonova kódu  $\mathbf{C}_q(n, k)$  sestává z nějakých  $n$  hodnot polynomu  $f(X)$ , který je stupně  $< k$ . Tento polynom můžeme jednoznačně zpětně určit interpolací jeho libovolných  $k$  funkčních hodnot.
- ▶ Tedy Reed-Solomonův kód  $\mathbf{C}_q(n, k)$  může opravit až  $(n - k)/2 = (d - 1)/2$  chyb.

## Algebraické dekodování Reed-Solomonových kódů

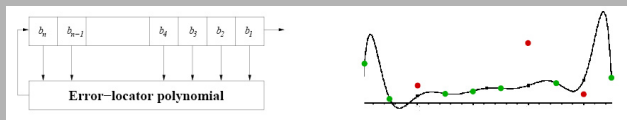
- ▶ Každé kódové slovo Reed-Solomonova kódu  $\mathbf{C}_q(n, k)$  sestává z nějakých  $n$  hodnot polynomu  $f(X)$ , který je stupně  $< k$ . Tento polynom můžeme jednoznačně zpětně určit interpolací jeho libovolných  $k$  funkčních hodnot.
- ▶ Tedy Reed-Solomonův kód  $\mathbf{C}_q(n, k)$  může opravit až  $(n - k)/2 = (d - 1)/2$  chyb.





## Algebraické dekódování Reed-Solomonových kódů

- ▶ Každé kódové slovo Reed-Solomonova kódu  $\mathbf{C}_q(n, k)$  sestává z nějakých  $n$  hodnot polynomu  $f(X)$ , který je stupně  $< k$ . Tento polynom můžeme jednoznačně zpětně určit interpolací jeho libovolných  $k$  funkčních hodnot.
- ▶ Tedy Reed-Solomonův kód  $\mathbf{C}_q(n, k)$  může opravit až  $(n - k)/2 = (d - 1)/2$  chyb.



- ▶ Berlekamp-Masseyho algoritmus je velmi efektivní způsob pro takovéto dekódování.

## **Algebraické soft-decision dekodování Reed-Solomonových kódů**

## Algebraické soft-decision dekódování Reed-Solomonových kódů

