

Samooperační kanál - kapacita kanálu, parametry kanálu, Shannova věta + inverz.

(téma) spolehlivá komunikace přes nespolehlivý kanál, kde?, za jakou cenu?
motivace: extraterestrické komunikace, CD+DVD, SSD disk, ...

komprese dat - odstranit redundanci → využít zpráv (ze záložnosti jejich distribuce)
vs. samooperační kanál - přidat redundanci, aby bylo možné poškozené zprávy rekonstruovat

$\sum_{y \in Y} p(y|x)$ $X \xrightarrow{\text{sum}} Y$ u.p. $X \dots$ odeslane' zpráva
 $y \dots$ přijata' zpráva $I(X,Y)$ jaké může být?

Prí: cela spolehlivý (bin.) kanál: $H(X|Y) = 0$

X $0 \longrightarrow 0$ Y $I(X,Y) = H(X) - H(X|Y) = H(X)$ max. pro $p(x) = (\frac{1}{2}, \frac{1}{2})$
 $1 \longrightarrow 1$ \Rightarrow kapacita $C = 1$ bit $(= 1 \text{ bit})$

Prí: cela nespolehlivý kanál: $H(X|Y) = H(X)$

$0 \xrightarrow{\frac{1}{2}} 0$ $I(X,Y) = 0$ pro všechny distribuce $p(x) \Rightarrow$ nahlodaj generátor
 $1 \xrightarrow{\frac{1}{2}} 1$ \Rightarrow kapacita $C = 0$

Prí: "semi-spolehlivý" (quad.) kanál: $H(X|Y) = 1$

$0 \xrightarrow{\frac{1}{2}} 0$ $I(X,Y) = H(X) - 1$ max. pro $p(x)$ uniform
 $1 \xrightarrow{\frac{1}{2}} 1$ \Rightarrow kapacita $C = \max_{p(x)} I(X,Y) = 1$ bit $(H(X) = 2)$
 $2 \xrightarrow{\frac{1}{2}} 2$
 $3 \xrightarrow{\frac{1}{2}} 3$ Jak spolehlivit přenos 1 bit?
1/2 výnade (typicky stejné, $X=Y=\{0,1\}$)

Def: kanál: $\langle X, p(y|x), Y \rangle$, kde $X, Y \dots$ vstupní, výstupní alfabety,

$p(y|x)$... matice pravd. pravd. ($\sum_j p(y|x) = 1$)

Kapacita kanálu: $C = \max_{p(x)} I(X,Y)$ t.j. přes vstupní distribuce

platí: $0 \leq C \leq \min(\log |X|, \log |Y|)$

Předpoklady na kanál:

• konečné vstupy a výstupy abecedy X, Y (diskretní)

• přenos jednotlivých symbolů navzájem nezávislé (bez paměti)

• vstupní bity nezávislí na výstupních symbolích (bez zpětné vazby)

$$\Rightarrow \left\| p(y^n|x^n) = \prod_{i=1}^n p(y_i|x_i) \right\|$$

Varianty: vypočítat, se záležitostmi, vzájemnou, spojitost, ...

Príklad: (bin.) symetrický kanál, p ... pravdepodobnosť chyby, $BUNO \leq p < 1/2$ gneč? (2)

$$I(X, Y) = H(X) - H(X|Y) = H(X) - \sum_j p(j) H(X|Y=j)$$

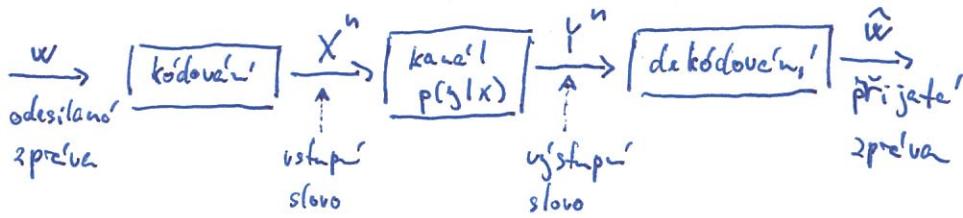
$$= H(X) - \sum_j p(j) H(p) = H(X) - H(p) \leq 1 - H(p)$$

rounost pravdepodobnosti uniformity \Rightarrow kapacita $C = 1 - H(p)$

(informačná) ponera informačné = kolik bitov čiame poslat / kolik jich poslali

[Dá sa dosiahnuť prímes informačnej prenosovej kapacity s libovolnou]
dĺžkou a pričom s informačnou ponierou ^{lib.} v blízkosti kapacity?

Vidme: ANS!! (pre bin. sym. kanál), pokial budeme kanál používať optimálne pre ponúkanú dostatočnosť všetkých dat



- zpráva $w \in W$... možnosť odberať zpráv, typicky $W = \{0, 1\}^k$
- $k = \lceil \log_2 |W| \rceil$... kolik bitov bychom chteli preniesť (pri uniformnej distribúcii zpráv)
- kód $f: W \rightarrow X^n$, typicky prosté, realizované napr. tabuľkou
- dĺžka kódu, stejne' pre všechny zprávy, závisí na posledovnosti prenosu
- kod f(W) = C = {c₁, ..., c_{|C|}} ⊆ Xⁿ, c_i ... kódovať slovo (napríklad s C s kódorom)
- dekódovať g: Yⁿ → W, (dešifračné tabuľky), závisí na volbe kódu C
- za predpokladu pravdepodobnosť chyby $p < 1/2$, abyže $g(g^n) = f^{-1}(D(g^n))$, kde $D: Y^n \rightarrow C$ je "najpodobnejšie" kódovať slovo (tzn. maximum-likelihood decoding)
- Hammingova vzdialenosť: $d_H(u, v) = |\{i \mid u_i \neq v_i\}|$ pro $u, v \in X^n$
- teda, $D(g^n) = c \Leftrightarrow d_H(g^n, c) = \min_{c' \in C} d_H(g^n, c')$ (teda t = g)
- $g(g^n) = \hat{w}$... prijaté zpráve

Ce požadujeme od kódu?

(3)

- a la Shannon: vysoká spolehlivost, tj. $\Pr[\text{gef}(\hat{c}) = c] \geq 1 - \epsilon$ (při uniform. distribuci zpráv)
- a la Hamming: detekovat / opravit lib. d chyb, tj. $D(\hat{c}) = c$ pro $d_H(c, \hat{c}) \leq d$

Př: opakovací kód: $(n, 1, n)_2$ -kód \rightarrow pomocí $R = 1/n$

$W = \{0, 1\}$, $C = \{0^n, 1^n\}$, $D(\hat{c})$... podle pravdějivého bitu (nachodné¹ pokud stejný, při n seude²)

$$\begin{aligned} \text{pravdějivá spolehlivost} &= \sum_{0 \leq i < n/2} \binom{n}{i} p^i (1-p)^{n-i} \rightarrow 1 \text{ pro } n \rightarrow \infty \quad (\text{bin. sym. kanał}) \\ &= (1-p)^3 + 3p(1-p)^2 \quad \text{pro } n=3 \\ p &\dots \text{pravd. chyba} \end{aligned}$$

- opraví lib.^{až} $(n-1)/2$ chyb, až počet $1/2$ opraví $n/2$ chyb, pro více chyb selže

Př: paritní kód: $(n, n-1, 2)_2$ -kód \rightarrow pomocí $R = \frac{n-1}{n}$

$W = \{0, 1\}^{n-1}$, $C = \{c \in \{0, 1\}^n \mid c_1 \oplus \dots \oplus c_n = 0\}$, $f(w) = w \underbrace{1 \oplus w_1 \oplus \dots \oplus w_{n-1}}_{\text{paritní bit}}$

$D(\hat{c}) = \hat{c}$ pokud se má parita, jinak zůstává nechápnutý bit

$$\text{pravdějivá spolehlivost} = (1-p)^n + p(1-p)^{n-1} \rightarrow 0 \text{ pro } n \rightarrow \infty$$

- detekuje 1 chybu, ale nemá (spolehlivě) opravit, pro více chyb selže

Def: Paritní kód C je $(n, k, d)_q$ -kód pokud pro kanál $\langle X, p(g|x), Y \rangle$:

n ... délka kódu, tj. $C \subseteq X^n$ (Pozn: [] závorky pro lineární kódy)

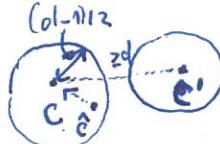
$$k = \lceil \log_2 |C| \rceil, \text{ (informační) pomocí } R = R(C) = \frac{k}{n} \quad (\text{alias " hustota" kódu})$$

$$d = d(C) = \min_{x_i, y_j \in C} d_H(x_i, y_j) \dots \text{ minimální vzdálenost}$$

$$q = |\mathcal{X}| = |\mathcal{Y}| \dots \text{velikost abecedy} \quad (\text{default } q=2)$$

$q_C(p) = \frac{1}{|C|} \sum_{c \in C} \Pr[D(\hat{c}) = c]$... spolehlivost kódu C při pravd. chyba p ,
tj. (antivráť) pomocí pravd. získaného slova \hat{c} je společně dešifrováno na vstupní

["Bin. kód minimální vzdálenost d umí detektovat libovolných $d/2$ chyb]
a opravit libovolných $(d-1)/2$ chyb.



$$B_n(c, (d-1)/2) \cap B_n(c', (d-1)/2) = \emptyset \quad \text{H. kóde disjunktní} \\ (\text{pro poloviční } d/2 \text{ se mohou dotýkat}) \quad \xrightarrow{\text{detektování}} \text{na nejbližší slovo}$$

Hammingova kóda se střídají s poloměrem r:

$$B_n(c, r) = \{w \in \{0, 1\}^n \mid d_H(w, c) \leq r\}$$

je OK

Pr: postat 100 bitů píš sgm. kanál s $p = 0.01 \Rightarrow$ kapacita $1-H(p) = 0.92$ (4)

a) bez kódovače: spolehlivost $(1-p)^{100} \approx 37\%$, power $R=1$

b) opakovací kód délky 3: $\left[(1-p)^3 + 3p(1-p)^2\right]^{100} \approx 97\%$, $R=1/3$

c) bloký délky 2, a $f(w_1, w_2) = (w_1, w_2, w_2, w_1 \oplus w_2)$

$D(\hat{c}) = \text{pravděpodobej. } \hat{c}_4 = w_1 \oplus w_2 \text{ je ok, z } \hat{c}_1, \hat{c}_2, \hat{c}_3 \text{ má. } w_1, w_2 \Rightarrow 1 \text{ chyba v paralelních řádcích budech}$

d) bloký délky 3, $f(w_1, w_2, w_3) = (w_1, w_2, w_3, w_1 \oplus w_2, w_2 \oplus w_3, w_1 \oplus w_3)$

číesci: kež dekodovat t.ž. opakovací lib. 1 chybu a v jidnou píš pohyb: 2 chyby
 \Rightarrow spolehlivost $\approx [(1-p)^6 + 6p(1-p)^5 + p^2(1-p)^4]^{100/3} \approx 95\%$, $R=1/2$

Vidíme: lepší power = horší spolehlivost, delší bloky → mohou poslat

Lze dekodovat několik kódů? Nejdřív posloužit fórum:

Turzov: Pro objem H. koule $V(n,r) = |\mathcal{B}_n(c_1, r)| = \sum_{i=0}^r \binom{n}{i}$ pro $0 < r \leq n/2$ platí

$$V(n,r) < 2^n H\left(\frac{r}{n}\right).$$

$$\text{Df: } 2^{nH\left(\frac{r}{n}\right)} = 2^{-r \log \frac{r}{n} - (n-r) \log \frac{n-r}{n}} = 2^{\log \frac{n^r}{r^r} \cdot \frac{n-r}{(n-r)^{n-r}}} = \frac{n^n}{r^r (n-r)^{n-r}}$$

$$n^n = (r + (n-r))^n = \sum_{i=0}^n \binom{n}{i} r^i (n-r)^{n-i} > \sum_{i=0}^r \binom{n}{i} r^r (n-r)^{n-r} \text{ pro } r \leq n/2 \quad \square$$

Věta (Černovova ner.): Nechť X_1, \dots, X_n mají různé n.p., $\Pr[X_i = 1] = p, \Pr[X_i = 0] = 1-p$

Pro každé $\alpha > 0$, $\Pr\left[\sum_{i=1}^n X_i \geq n(p+\alpha)\right] \leq e^{-\frac{n\alpha^2}{2}}$. \square

Df: viz např. sfraňka k pravděsíce, souhru pravd. \square

Diskledek: # chyb píš pravděsí sgm. kanálem bude o intervalu

$[n(p-1), n(p+\alpha)]$ s pravd. aspoň $1 - 2e^{-\frac{n\alpha^2}{2}}$. (tj. sítě koncentruje kolmo $E[\sum X_i] = np$)

Df: $X'_i = \begin{cases} 1 & \text{j. chyba} \\ 0 & \text{j. náh.} \end{cases}$, $X'_i = 1 - X_i$, z náh. pro X'_i a pro X_i

$$\Pr[\sum X'_i \leq n(p-\alpha)] = \Pr[\sum X'_i \geq n(1-p+\alpha)] \leq e^{-\frac{n\alpha^2}{2}}. \quad \square$$

Věta (Shannon): Pro $0 < p < 1/2$, $R < 1 - H(p)$, $\varepsilon > 0$ existuje kód C pro (5) sym. kanál \rightarrow použití $R(C) \geq R$ a spolehlivost $P_C(p) \geq 1 - \varepsilon$.

D2: Pro dostatečnou velkou n (upřesně podle ji) na "hodě" (vezměte uniformní) uživatelského slova 2^{Rn} slov (kód C) $\geq 80,13^n$. Chápe $P_C(p) \geq 1 - \varepsilon$.

- na "hodě" procesy:
 - volba kódu C
 - průpis vstupního slova c na užívání \hat{c}

když máme vzdálost dle ban: $d_h(\hat{c}, x) \leq d_h(\hat{c}, c)$ pro nejake $x \in C \setminus \{c\}$.

- Umožně: $B_n(\hat{c}, r)$ skoro jistě obsahuje c a žádoucí jiné $x \in C$ při vhodné zvolení parametru r .

$$\text{Definice: } \hat{c} = \min_{x \in C \setminus \{c\}} d_h(\hat{c}, x)$$

Nechť $r = n(p+2)$, kde $\lambda > 0$ t.ž. $H(p+2) + R < 1$ (tře).

$$a) P_1 := P_n[c \notin B_n(\hat{c}, r)] \leq e^{-n\lambda^2/2} \quad (\text{dle Bern. ner.})$$

$$b) \text{ pro } x \in C \setminus \{c\} \quad P_n[x \in B_n(\hat{c}, r)] = \frac{V(n, r)}{2^n} \quad (\text{dle výpočtu}) \\ \leq \frac{2^n H(\frac{r}{n}) - n}{2^n} = 2^{n(H(p+2) - 1)} \quad (\text{dle Bern.})$$

Tedy platí $P_1 \approx 0$ a $B_n(\hat{c}, r)$ je nejake $x \in C \setminus \{c\}$:

$$P_2 \leq 2^{Rn} \cdot 2^{n(H(p+2) - 1)} = 2^{n(H(p+2) + R - 1)}$$

$\Rightarrow \lambda$ je velký, $P_1 + P_2$ klesejí s λ a vzdáleností n , Nechť n dostatečnou velkou, aby $P_1 + P_2 \leq \varepsilon$. Pak $P_C(p) \geq 1 - \varepsilon$. \square

Pozn: platí: pro jiný kanál, volbu kódů vzhledem k optimální distribuci pro kapacitu.

\Rightarrow kapacita kanálu se může libovolně zvětšit \rightarrow libovolnou velkou spolehlivostí přenosu (polohu dovolené "velké" dat).

\Rightarrow Můžeme ji překročit? NE! Respektive ano, ale jen s omezenou spolehlivostí (polohu chyb přenese libovolná data), viz následující výkaz.

\Rightarrow [kapacita kanálu je hranice po spolehlivém přenosu informace.]
(ve shodě s intuicí).

Veta ("inverzní"): P_{ch} $0 < p < 1/2$, $R > 1 - H(p)$, $\epsilon > 0$ existuje n t.z. každý kód C (pro sym. kanál) dleky aspoň n → posílení $R(c) \geq R$ má spolehlivost $S_c(p) \leq \epsilon$.

Dl.: Spolu. Nechť pro nejake' $\epsilon > 0$, $R > 1 - H(p)$ existuje libovolná dleky kód C s posílením aspoň R a spolehlivostí aspoň ϵ . Označme D jeho dekódovací fc.

- idea:
 - vymeď $d_h(\hat{c}, c) \in [u(p-1), u(p+1)]$ stále jistě
 - velká spolehlivost \Rightarrow hodně slov \hat{c} se opraví (správně) na c
 - slov je n 2ⁿ, každá dekódují unikátně \Rightarrow kód nemůže být velký. G (posílení $R > 1 - H(p)$)

Nechť $\alpha > 0$ t.z. $H(p) + R - \alpha \log \frac{1-p}{p} > 1$ (1x).

$$S(c) = \{u \in \{0,1\}^n \mid u(p-1) \leq d_h(u, c) \leq u(p+1)\} \dots \text{prstence okolo } c$$

a) $\Pr[\hat{c} \in S(c)] \geq 1 - \epsilon/2$ pro dostatečně velké n (dle Čern. ner.)

b) $\sum_{c \in C} \Pr[\hat{c} \in \tilde{D}(c)] \geq |C| \cdot \epsilon \geq 2^{Rn} \cdot \epsilon$ (dle spolehlivosti $\approx \epsilon$) a posílení $R(c) \geq R$ (Pr[A ∩ B] ≥ Pr[A] +

slova, která se dekódují na c)

c) $\sum_{c \in C} \Pr[\hat{c} \in \tilde{D}(c) \cap S(c)] \geq \sum_{c \in C} (\Pr[\hat{c} \in \tilde{D}(c)] + \Pr[\hat{c} \in S(c)] - 1) \quad \Pr[B] - 1$

u kolik slov z prstence okolo c
se správně opraví na c

$\geq \sum_{c \in C} (\Pr[\hat{c} \in \tilde{D}(c)] - \epsilon/2) \geq 2^{Rn} \cdot \frac{\epsilon}{2} \quad \text{dle a), b)}$

$= \sum_c \sum_{x \in \tilde{D}(c) \cap S(c)} \Pr[\hat{c} = x]$

d) Aby $\hat{c} = x$ pro $x \in S(c)$, musí nastat aspoň $u(p-1)$ chyb.

$$\Pr[\hat{c} = x] \leq p^{u(p-1)} \cdot (1-p)^{u(1-p+1)} \quad \text{neboť } p < 1/2 \text{ a } d_h(\hat{c}, x) \geq u(p-1).$$

$$= p^{u(p-1)} \cdot \left(\frac{1-p}{p}\right)^{u(1-p+1)} = 2^{-uH(p)} \left(\frac{1-p}{p}\right)^{u(1-p+1)}$$

e) Výdělením e) a d),

$$2^n = \sum_{c \in C} |\tilde{D}(c)| \geq \sum_{c \in C} |\tilde{D}(c) \cap S(c)| \geq \frac{2^{Rn} \cdot \epsilon/2}{2^{-uH(p)} \left(\frac{1-p}{p}\right)^{u(1-p+1)}} = 2^n \underbrace{(H(p) + R - \alpha \log \frac{1-p}{p} + \frac{\log \epsilon/2}{n})}_{> 1} \quad \text{jde k 0 (zepředu)}$$

$$> 2^n \text{ pro dostatečně velké n. G. } \square$$