- Huffmanův kód je citlivý na chybu v distribuci

- Přibližně existuje univerzální kód rychlosti $R$ bitů/papír zdroj s entropií $H(X) < R$

- Idea: Existuje $2^{nH(P)}$ posloupností typu $P$.
  Pro dost velké $n$ je počet možných typů menší než počet posloupností $\vec{x} \in X^n$ s typem $P_{\vec{x}}$ pro které $H(P_{\vec{x}}) < R$ bitů, vyjádřím $< nR$ bitů.
  Tedy množina má velkou pravděpodobnost.

Definice: Blokový kód rychlosti $R$ bitů/znak. Nechť $X_1, X_2, \dots X_n$ s neznámou distribucí $Q$ se skládá ze dvou zobrazení:

Kodér
$$\varphi_n : X^n \to \{1, 2, 3, \dots, 2^{\lfloor nR \rfloor}\}$$

a dekodér
$$\psi_n : \{1, 2, \dots, 2^{\lfloor nR \rfloor}\} \to X^n$$

Pravděpodobnost chyby vzhledem k distribuci $Q$ je

$$P_e^{(n)} = Q^n\left(\{\vec{x} \in X^n \mid \varphi_n(f_n(\vec{x})) \neq \vec{x}\}\right)$$

Takový kód se nazývá univerzální, jestliže funkce $f_n$ a $\varphi_n$ nezávisí na $Q$ a platí

$$P_e^{(n)} \to 0 \quad \text{pro } n \to \infty \quad \text{právě když } R > H(Q).$$

---

**Věta:** Existuje posloupnost $(2^{nR}, n)$ univerzálních asymptotických kódů taková, že

$$P_e^{(n)} \to 0 \quad \text{pro každý zdroj } Q \text{ s } H(Q) < R.$$

**Důk:** $R > 0$

$$R_n = R - |X| \cdot \frac{\log(n+1)}{n}$$

Uvažme množinu

$$A_n = \{\vec{x} \in X^n : H(P_{\vec{x}}) \leq R_n\}.$$

Odhadněme její velikost

$$|A_n| = \sum_{\langle P \in \mathcal{P}_n \mid H(P) \le R_n \rangle} |T(P)| \le$$

$$\le \sum_{\langle P \in \mathcal{P}_n \mid H(P) \le R_n \rangle} 2^{nH(P)}$$

$$\le \sum_{\langle P \in \mathcal{P}_n \mid H(P) \le R_n \rangle} 2^{nR_n} \le (n+1)^{|\mathcal{X}|} \cdot 2^{nR_n} = 2^{nR}$$

↓ ne skalárnost ostrá nerovnost

Kodér očíslujme posloupnosti v $A_n$

$$A_n = \langle \vec{x}_1, \vec{x}_2, \dots, \vec{x}_\ell \rangle, \quad \ell < 2^{nR}$$

Kodér: $f_n(\vec{x}) = \begin{cases} f_n(\vec{x}_i) = i, & 1 \le i \le \ell \\ f_n(\vec{x}) = \ell & \vec{x} \notin A_n \end{cases}$

dekodér

$$\varphi_n(i) = \vec{x}_i, \quad 1 \le i \le \ell$$

$\varphi_n \circ f_n$ funguje dobře na $A_n$

$$P_e^{(n)} \le 1 - Q^n(A_n)$$

$$= \sum_{\langle P \in \mathcal{P}_n : H(P) > R_n \rangle} Q^n(T(P)) \le$$

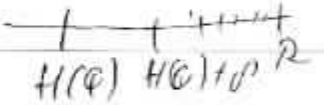
$$\le (n+1)^{|\mathcal{X}|} \cdot \max_{\langle P \in \mathcal{P}_n : H(P) > R_n \rangle} Q^n(T(P))$$

$$\le (n+1)^{|\mathcal{X}|} \cdot 2^{-n \min_{\langle P \in \mathcal{P}_n ; H(P) > R_n \rangle} D(P\|Q)}$$

Označme $H_n = \min_{\langle P \in \mathcal{P}_n \mid H(P) > R_n \rangle} D(P\|Q)$

$R_n \nearrow R$; tudíž existuje $n_0$ tak, že

(+) $R_n > H(Q) + \delta$, $\forall n \ge n_0$, pro nějaké $\delta > 0$




Ukážeme, že existuje $c > 0$ tak, že

$$H_n > c \quad \forall n \ge n_0$$

Kdyby ne, pak existuje posl. $P_{n_k} \in \mathcal{P}_{n_k}$,
$H(P_{n_k}) > R_{n_k} > H(Q) + \delta$
tak, že $D(P_{n_k}\|Q) \xrightarrow[n_k \to \infty]{} 0$

Pak dle Pinskera a spol.

$$H(P_{n_k}) \xrightarrow[n_k \to \infty]{} H(Q) \quad \text{- spor s (+)}.$$

**Tvrzení:** Pinskerova nerovnost

$\mathcal{X}$ - konečná
$P, Q$ - distribuce na $\mathcal{X}$

Pak

$$D(P\|Q) \geq \frac{1}{2}\left(\sum_{x\in\mathcal{X}} |P(x)-Q(x)|\right)^2$$

**Důsledky:** Máme-li posloupnost distribucí $P_n$ takových, že $D(P_n\|Q) \xrightarrow[n\to\infty]{} 0$,

pak $\lim_{n\to\infty} P_n(x) = Q(x) \quad \forall x\in\mathcal{X}$

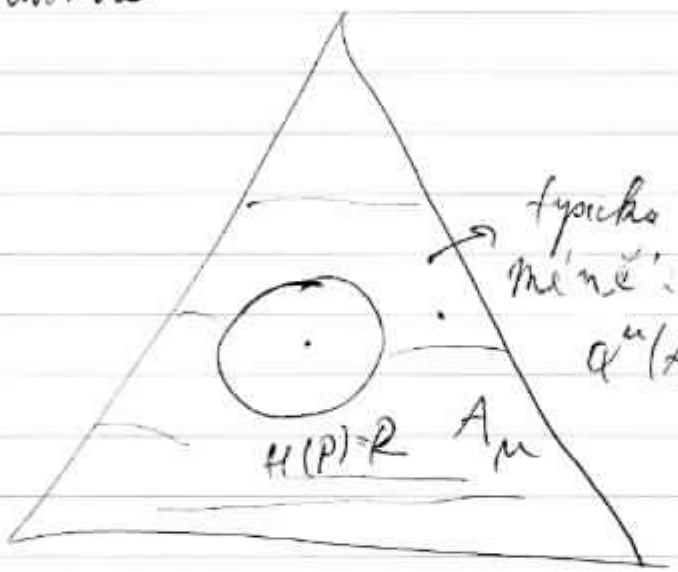
a $\lim_{n\to\infty} H(P_n) = H(Q)$.

Máme tedy odhad

$$P_e^{(n)} \leq (n+1)^{|\mathcal{X}|} \cdot 2^{-nc} \longrightarrow 0 \quad (n \to \infty)$$

---

Ilustrace




jinak $\mathcal{X}$ prvků
$|\mathcal{X}|^n = 2^{n \log |\mathcal{X}|}$
ale nyní $n$
s problémem $|\mathcal{X}| \gg 2$.

Lempel-Ziv algoritmus (zdroj s pamětí)

- dva klíčové články 1977, 1978

L77 - posouvající se okno
L78 - "stromový" algoritmus

L78: popis (binární případ)

- budeme slovník ve tvaru stromu, kde uzly odpovídají řetězcům dosud viděným.
- zdrojovou posloupnost se očíslkuje (parsuje) tak, že se vždy vezme nejdelší řetězec, který tu ještě nebyl

A|B|BA|BB|AB|BBA|ABA|BAA

A, B, BA, BB, AB, BBA, ABA, BAA

každé číslo je o jeden znak delší než předchozí — dáme kód předpony a poslední znak

(0,A); (0,B), (2,A), (2,B), (1,B), (4,A)

nebyl (5,A), (3,A).

(Unix, modemy, GIF)

množiny řeky za sebou

$c(n)$ ... počet různých posloupností délky $n$

velikost kódu

$$c(n)\lceil \log c(n) + 1 \rceil$$

↓ ↓

pointer k ostatním

---

Věta Je-li $(X_n)_{n=1}^{\infty}$ binární stacionární ergodický zdroj s nulovou entropií $H(\mathbb{X})$, pak

$$\limsup_{n\to\infty} \frac{c(n)\log c(n)}{n} \leq H(\mathbb{X})$$

s pravděpodobností 1.

---

# Kapacita informačních kanálů

Informační kanál modeluje prostředí (šum)

vstupní pravděpodobnost → [prostředí matice přechodu] → výstup

**Definice** Trojice $K = (X, p(y|x), Y)$ kde $X, Y$ je vstupní a výstupní abeceda a $p(y|x)$ je systém podmíněných pravděp. se nazývá informační kanál | často $X = Y$

$\pi(x) = 1 - p(x|x)$ – pravděp. chyby

**Bezšumový kanál:** pro všechny zdroje $\Leftrightarrow$ $H(X) = I(X,X) = I(X,Y)$

$\Leftrightarrow$ každý řádek přech. matice je Diracův vůči $Y \in X$

$= H(X) - H(X|Y)$

**Definice** Informační kapacita kanálu

$$C(K) = \sup_{p(x)} \underline{I}(X;Y)$$

kde supremum se bere přes všechny možné rozdělení $(x, p(x))$.

Supremum je maximum: $\underline{I}(X,Y)$ je spojitá funkce a množina distribucí je uzavřená omezená množina (prostředek simplex). Tedy existuje maximum.

Vlastnosti kapacity:

1. $C \geq 0$ neboť $\underline{I}(X,Y) \geq 0$

2. $C \leq \log|\mathcal{X}|$ neboť $C = \max \underline{I}(X,Y) \leq \max H(X)$
   $\leq \log|\mathcal{Y}|$ $= \log|\mathcal{X}|$

3. $\underline{I}(X,Y)$ je spojitá funkce $p(x)$

4. $\underline{I}(X,Y)$ je konkávní funkce $p(x)$
   $\Rightarrow$ lokální maximum je globální maximum

Hledání: Kuhn-Tucker, gradientní metoda

často platí, že $p(\cdot|x_1)$ a $p(\cdot|x_2)$ se liší pouze permutací prvků pořadnosti.
Pak $H(Y|x_1) = H(Y|x_2)$. Pak pro podmíněnou entropii platí

$$H(Y|X) = \sum_{x \in X} H(Y|x)\, p(x) = H(Y|x)$$

(nezávisí na rozdělení $p(x)$)

$$C(K) = \max_{p(x)} I(X;Y) = \max_{p(x)} [H(Y) - H(Y|x)]$$

$$= \max_{p(x)} H(Y) - H(Y|x) \quad (x \in X \text{ libovolné})$$

Příklad: Binární bezšumový kanál

$$K = (\{0,1\}, p(y|x), \{0,1\})$$

$$p(y|x) = \delta_x(y)$$

$p(0) = \bar{u}$ $\quad 0 \xrightarrow{1} 0$

$1 \xrightarrow{1} 1$

$p(1) = 1 - \bar{u}$

Podmínka je splněna $H(Y|x) = 0 \ \forall x \in X$

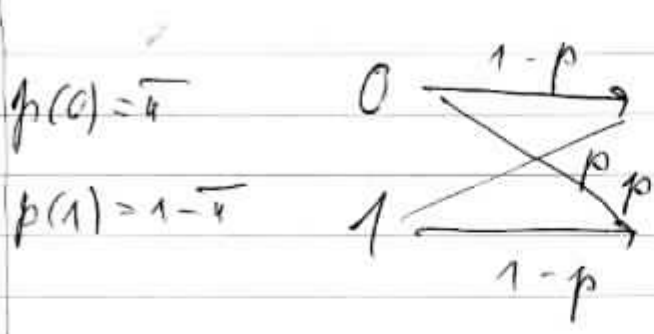
$$C(K) = \max_{0 \le \bar{u} \le 1} H(Y) - 0 = \max_{0 \le \bar{u} \le 1} H(\bar{u}, 1-\bar{u})$$

$$= 1$$

pro $\bar{u} = 1/2$ tj. 1 bit/znak

Binární kanál $K$ se nazývá <u>symetrický</u> jestliže

$$p(y|u) = p(u|y) \quad \forall u, y \in \mathbb{Z}_2$$




BSK(p)

matice přechodu

$$\begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}$$

$$C(K) = \max_{0 \le \bar{u} \le 1} H(Y) - h(p) =$$

$$= \max_{0 \le \bar{u} \le 1} H(\bar{u}(1-p) + (1-\bar{u})p,\ \bar{u}p + (1-\bar{u})(1-p)) - h(p)$$

$$= \max_{0 \le \bar{u} \le 1} h(\bar{u}(1-p) + (1-\bar{u})p) - h(p)$$

$$=$$

$$\bar{u} = 1/2 \quad h(1/2) - h(p) = 1 - h(p)$$

maximální kapacita pro $p = 0, 1$ bude 1 (dokonalý kanál)

Bude-li $p$ blížit k $1/2$ bude se kapacita blížit k 0.

Pro $p > 1/2$ je vstup a výstup statisticky nezávislý!

Příklad: Binární kanál se ztrátou

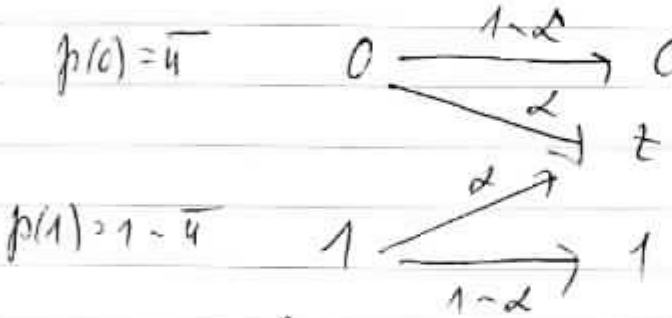
x definovaný jako | BKZ(p) |

$K = (\langle 0,1\rangle, p(y|x), \langle 0,1,Z\rangle)$

kde

$p(y|x) = p(z|x) = 1-\alpha$ $\quad \alpha \in \langle 0,1)$

$p(z|x) = p(z|y) = \alpha$




opět platí nezáměnnost $H(Y|x)$ na $x$

$H(Y|x) = H(1-\alpha, 0, \alpha) = h(\alpha)$

$C(K) = \sup_{0 \le \bar{\pi} \le 1} H(Y) - h(\alpha)$

$= \sup_{0 \le \bar{\pi} \le 1} H(\bar{\pi}(1-\alpha), \alpha, (1-\bar{\pi})(1-\alpha)) - h(\alpha)$ ← pro ztrátu

$H(\bar{\pi}(1-\alpha), \alpha, (1-\bar{\pi})(1-\alpha)) =$

$= \bar{\pi}(1-\alpha)[-\log \bar{\pi} - \log(1-\alpha)]$

$- \alpha \log \alpha$

$+ (1-\bar{\pi})(1-\alpha)[-\log(1-\bar{\pi}) - \log(1-\alpha)]$

$= h(\alpha) + (1-\alpha) h(\bar{\pi})$

Tedy

$$C(K) = \sup_{0 \le u \le 1} (1-\alpha) h(u) = \sum_{u=1}^{1-\alpha}$$

ukazuje se, že záměna znaků méně omezuje kapacitu binárního kanálu než záměna symbolů.
Konkrétně

BKZ(2p) má větší kapacitu než BSK(p)

pro $0 \le p < 1/2$ $\quad 1-2p > 1-h(p)$

tj. $h(p) > 2p$ ; $0 < p < 1/2$

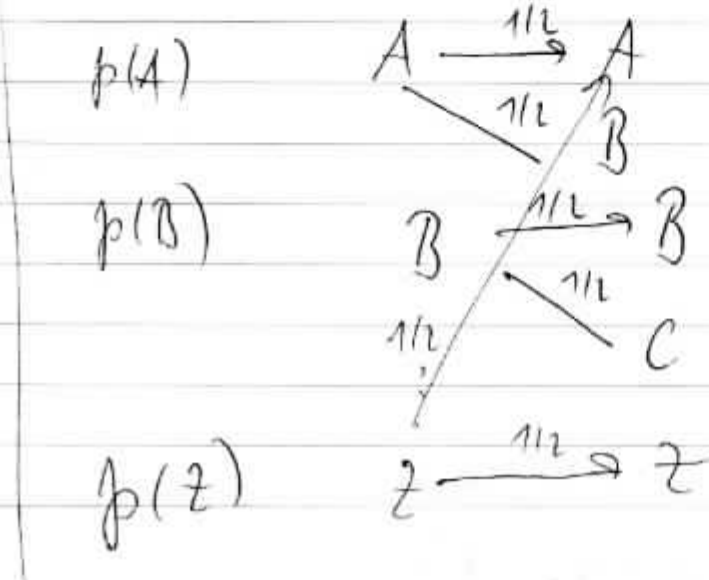
dle konkávity $h$ : $\alpha = 1-2p$

$$h(p) > \alpha h(0) + (1-\alpha) h(1/2) = 1-\alpha = 2p$$

cenný praktický význam mají při radiové komunikaci.

---

Příklad: Ternární posloupnost



Všechny podmíněné entropie jsou nulové

$H(1|2) = 0$

$$C(K) = \sup_{p(x)} H(Y) - 1 = \sup_{p(x)} H\left(\frac{p(A)+p(D)}{2}, \frac{p(Z)+p(A')}{2}\right) - 1$$

$$= H\left(\frac{1}{26}, \frac{1}{26}, \dots, \frac{1}{26}\right) - 1 = \log 26 - 1 = \log 13.$$

$p = (\underbrace{\frac{1}{26}, \dots}_{\text{harmonické}})$