

## 8 ÚROVEŇ ZDROJ INFORMÁCIE - PRIJÍMAČ INFORMÁCIE

V tejto kapitole budeme sledovať prenos informácie bez ohľadu na to, aké transformácie signálu sa robia v informačnom reťazci. Budeme študovať vlastnosti základného informačného reťazca: zdroj informácie - kanál - prijímač informácie z pravdepodobnostného hľadiska v rámci Shannonovej teórie informácie.

### Definícia:

Nech je daná konečná množina  $X = \{x_0, x_1, \dots, x_{M-1}\}$ , ktorú nazveme abecedou a pravdepodobnostný priestor  $(X, \Omega, P)$ . Diskrétnym stacionárnym zdrojom informácie nazývame zariadenie, ktoré za každú časovú jednotku vygeneruje náhodnú správu  $u \in \Omega$ .

### Definícia:

Diskrétny stacionárny zdroj informácie  $(X, \Omega, P)$  (označíme  $(X^N, P)$ ) a nazveme zdrojom s dĺžkou slova  $N$ , ak každá správa je  $u \in X^N$ , t.j.

$$u = (u_0, u_1, \dots, u_{N-1}), \quad u_i \in X, \quad i = 0, 1, \dots, N-1$$

kde  $N$  je prirodzené číslo.

Diskrétny stacionárny zdroj informácie  $(X, \Omega, P)$  nazveme Markovovým, ak pre každú správu  $u = (u_0, \dots, u_{N-1}) \in \Omega$  platí

$$p(u_{N-1}/u_{N-2}) = p(u_{N-1}/u_{N-2}, \dots, u_0)$$

Diskrétny stacionárny zdroj informácie  $(X, \Omega, P)$  nazveme bez pamäte, ak pre každú správu  $u = (u_0, \dots, u_{N-1}) \in \Omega$

$$p(u_{N-1}) = p(u_{N-1}/u_{N-2}, \dots, u_0)$$

V ďalšom texte pod zdrojom informácie budeme rozumieť diskrétny stacionárny zdroj informácie s dĺžkou slova  $N$ .

### 8.1 VZÁJOMNÁ INFORMÁCIA

#### Definícia:

Veličinu  $J(y, x)$ , budeme nazývať informáciou o jave  $y \in Y$ , ktorá je obsiahnutá v jave  $x \in X$ , ak platí:

1. v pravdepodobnostnom priestore  $(X \times Y, \Omega, P)$  je  $J(y, x)$  diferencovateľnou funkciou  $F(\psi, \theta)$  dvoch premenných  $\psi = P(y)$ ,  $\theta = P(y/x)$ .
2. v pravdepodobnostnom priestore  $(X \times Y \times Z, \Omega, P)$  je  $J(y, x/z)$  tou istou funkciou  $F(\psi, \theta)$  premenných  $\psi = P(y/Z)$ ,  $\theta = P(y/xz)$
3. v pravdepodobnostnom priestore  $(X \times Y \times Z, \Omega, P)$  platí

$$J(y, xz) = J(y, z) + J(y, x/z)$$

4. v pravdepodobnostnom priestore  $(X \times Y \times U \times V, \Omega, P)$ , v ktorom

$$P(xyuv) = P(xy) \cdot P(uv)$$

platí

$$J(xu, yv) = J(x, y) + J(u, v)$$

Dá sa ukázať [6], že až na multiplikatívnu konštantu (ktorá tiež súvisí so základom logaritmu) vyhovuje danej definícii len funkcia

$$J(y, x) = \log \frac{p(y/x)}{p(y)} \quad (1)$$

Vzájomnú informáciu

$$\psi(y, x/z) = \log \frac{p(y/xz)}{p(y/z)}$$

voláme podmienenou vzájomnou informáciou.

Pri použití dvojkového logaritmu nazývame jednotku informácie Shannon v skratke [Sh].

Presvedčte sa, že vzájomná informácia podľa (1) skutočne vyhovuje požiadavkám 3., 4. definície.

Vzájomná informácia je reálne číslo, pričom

$$J(y, x) \begin{cases} > 0 & \text{pre } p(y/x) > p(y) \\ = 0 & \text{pre } p(y/x) = p(y) \\ < 0 & \text{pre } p(y/x) < p(y) \end{cases}$$

Veta:

Vzájomná informácia je symetrická funkcia.

Dôkaz:

$$J(y, x) = \log \frac{P(y/x)}{P(y)} = \log \frac{P(xy)}{P(x)P(y)} = \log \frac{P(x/y)}{P(x)} = J(x, y)$$

pre

$$p(x) = 0, \quad p(y) \neq 0$$

Jednoduchými úpravami dostaneme tiež vzťah

$$J(yz, x) = J(x, yz) = J(z, x) + J(y, x/z)$$

Ak nastatie javu  $x$  úplne podmieňuje nastatie javu  $y$ , t.j.

$$P(y/x) = 1$$

potom platí

$$J(y, x) = J(y) = \log \frac{1}{P(y)}$$

Veličinu  $J(y)$  voláme úplnou informáciou o jave  $y$ . Pretože  $P(y/x) \leq 1$  a z podmienky symetrie vyplýva

$$J(x, y) \leq J(x)$$

$$J(x, y) \leq J(y)$$

Podmienenou úplnou informáciou voláme veličinu

$$J(y/z) = \log \frac{1}{P(y/z)}$$

Pre vzájomnú informáciu môžeme potom písať

$$J(y, x) = J(y) - J(y/x)$$

resp.

$$J(y, x) = J(y) + J(x) - J(xy)$$

Odtiaľ pre úplnú informáciu o súčasnom nastatí javov  $xy$

$$J(xy) = J(x) + J(y) - J(y, x)$$

## 8.2 STREDNÁ HODNOTA INFORMÁCIE

Vzájomná informácia  $J(y, x)$  je náhodnou veličinou v pravdepodobnostnom priestore  $(X \times Y, \Omega, P)$ . Môžeme ju charakterizovať číselnými charakteristikami, z ktorých najjednoduchšou je stredná hodnota.

Strednú hodnotu

$$J(Y, x) = \sum_{y \in Y} p(y/x) J(y, x)$$

budeme volať informáciou o systéme javov  $Y$ , ktorá je v jave  $x$ .

Veta:

Platí

$$J(Y, x) \geq 0$$

Dôkaz

$$J(Y, x) = \sum_{y \in Y} p(y/x) \log \frac{p(y/x)}{p(y)}$$

resp.

$$- J(Y, x) = \sum_{y \in Y} p(y/x) \ln \frac{p(y)}{p(y/x)} \log e$$

použitím nerovnosti

$$\ln x \leq x - 1$$

dostávame

$$- J(Y, x) \leq \sum_{y \in Y} p(y/x) \left[ \frac{p(y)}{p(y/x)} - 1 \right] \log e$$

čo so vzťahmi

$$\sum_{y \in Y} p(y) = 1, \quad \sum_{y \in Y} p(y/x) = 1$$

dáva

$$- J(Y, x) \leq 0$$

Strednú hodnotu

$$J(y, X) = \sum_{x \in X} p(x) \log \frac{p(y/x)}{p(y)}$$

voláme informáciou o jave  $y$ , ktorá je obsiahnutá v systéme javov  $X$ . Z vlastnosti symetrie vzájomnej informácie plynie

$$J(y, X) \geq 0$$

Strednú hodnotu

$$J(Y, X) = \sum_{x \in X} p(x) \quad J(Y, x) = \sum_{y \in Y} p(y/x) \quad J(y, X)$$

voláme informáciou o systéme javov  $Y$ , ktorá je obsiahnutá v systéme javov  $X$ . Po dosadení za  $J(Y, x)$ , resp.  $J(y, X)$  dostávame

$$J(Y, X) = \sum_{(x, y) \in X \times Y} p(xy) \log \frac{p(y/x)}{p(y)}$$

Je zrejmé, že platí

$$J(Y, X) \geq 0.$$

Rovnosť platí práve vtedy, keď  $p(xy) = p(x) p(y)$  pre všetky  $(x, y) \in X \times Y$ , t.j. javy  $x, y$  sú nezávislé.

### 8.3 ENTROPIA

Tak ako sme definovali strednú hodnotu vzájomnej informácie, budeme definovať aj strednú hodnotu úplnej informácie, ktorú voláme entropiou.

Definícia:

Nech je daný pravdepodobnostný priestor  $(X, \Omega, P)$ , resp.  $(X \times Y, \Omega, P)$ . Strednú hodnotu úplnej informácie

$$H(X) = \sum_{x \in X} p(x) \log \frac{1}{p(x)} \quad (1)$$

resp.

$$H(X/Y) = \sum_{(x, y) \in X \times Y} p(x, y) \log \frac{1}{p(x/y)} \quad (2)$$

voláme entropiou, resp. podmienenou entropiou systému javov  $X$ .

Veta:

$$\text{Ak } X = \{x_0, x_1, \dots, x_{M-1}\}, \text{ potom} \\ 0 \leq H(x) \leq \log M$$

Dôkaz:

Ľavá nerovnosť vyplýva z toho, že v sume (1) sú všetky sčítance nezáporné. Rovnosť na ľavej strane nastáva, ak



$$p(x_i) = \begin{cases} 1, & i = j \quad i = 0, 1, \dots, M-1 \\ 0, & i \neq j \quad j \in \{0, 1, \dots, M-1\} \end{cases}$$

pretože  $\lim_{p \rightarrow 0} p \log p = 0$ .

Nerovnosť na pravej strane dokážeme dôkazom nerovnosti

$$H(x) - \log M \leq 0$$

pomocou nerovnosti

$$\ln x \leq x-1$$

rovnako ako v prípade dôkazu nerovnosti  $J(Y, x) \geq 0$ .

Rovnako je možné dokázať aj vzťah

$$H(X/Y) \leq H(X) \quad (3)$$

kde rovnosť nastáva, ak  $X$  a  $Y$  sú systémy nezávislých javov. Rozpísaním logaritmov a pravdepodobnosti súčasného nastatia dvoch javov dostaneme

$$H(XY) = H(X) + H(Y/x) = H(Y) + H(X/Y) \quad (4)$$

a dôležitý vzťah

$$J(Y, X) = H(Y) - H(Y/X) \quad (5)$$

Doporučujeme čitateľovi, aby tieto vzťahy dokázal.

#### 8.4 ZDROJ INFORMÁCIE

Stacionárny diskretný zdroj informácie sme definovali v úvode kap. 8. Z informačného hľadiska budeme výdatnosť zdroja hodnotiť stredným množstvom informácie v jednom symbole, ktorý zdroj informácie vygeneroval. Vo všeobecnosti sú však generované symboly na sebe závislé. Ak zdroj informácie  $(X^N, P)$  generuje správy o dĺžke  $N$ , potom informačná výdatnosť stacionárneho zdroja bude  $H(X^N)/N$ . Podľa vzťahu (8.3.4) platí

$$H(X^N) = H(X^{N-1}) + H(X_N/X^{N-1})$$

kde  $X^N = X \times X \times \dots \times X$  je  $N$ -násobný kartézsky súčin a  $X_N$  je abeceda zdroja informácie v čase  $i=N$ . Čas uvádzame len kvôli lepšej orientácii, je zrejmé, že pre stacionárny zdroj, ktorý v tomto texte predpokladáme, platí

$$X_i = X, \quad i = 1, \dots, N$$

Hodnota  $H(X_N/X^{N-1})$  udáva stredné množstvo informácie v symbole  $u_N$  správy  $u = (u_1, \dots, u_N)$  za podmienky, že časť tejto správy  $(u_1, \dots, u_{N-1})$  je známa. Nasledujúca veta tvrdí, že toto množstvo s rastúcim  $N$  konverguje.

Veta:

Pre každý diskretný stacionárny zdroj existuje limita

$$H(X/X^\infty) = \lim_{N \rightarrow \infty} H(X_N/X^{N-1})$$

Dôkaz:

Ukážeme, že postupnosť

$$H(X_1), H(X_2/X_1), \dots, H(X_N/X_{N-1} \dots X_1)$$

nerastie. Pre stacionárny zdroj sa uvedená postupnosť rovná postupnosti

$$H(X_N), H(X_N/X_{N-1}), \dots, H(X_{N-1}, \dots, X_1)$$

a táto je podľa (8.3.3) nerastúca.

Okrem toho členy postupnosti sú ohraničené zdola

$$H(X_N/X_{N-1}, \dots, X_1) \geq 0$$

Pretože každá monotónna postupnosť má limitu, bude ju mať aj uvedená postupnosť a ako sme už ukázali, bude konečná.

Ak informačnú výdatnosť zdroja  $(X^N, P)$  označíme

$$H_N(X) = \frac{H(X^N)}{N}$$

potom pre rastúce  $N \rightarrow \infty$  konverguje.

Veta:

Pre každý stacionárny diskretný zdroj existuje limita

$$\lim_{N \rightarrow \infty} H_N(X) = \lim_{N \rightarrow \infty} H(X_N/X^{N-1}) = H(X/X^\infty)$$

Dôkaz:

Ukážeme najskôr, že limita existuje. Z (8.3.4) a (8.3.3) vyplýva

$$H(X^{N+1}) = H(X^N) + H(X_{N+1}/X^N) \leq H(X^N) + H(X_N/X^{N-1}) \quad (1)$$

Zovšeobecnením vzťahu (8.3.4) dostávame

$$H(X^N) = \sum_{i=1}^N H(X_i/X^{i-1})$$

a pretože podľa (8.3.3)

$$H(X_N/X^{N-1}) \leq H(X_1/X^{1-1}), \quad i = 1, 2, \dots, N$$

kde  $H(X_1/X_0) = H(X_1)$ , platí

$$H(X^N) \geq NH(X_N/X^{N-1})$$

Spolu s nerovnosťou (1) dostávame

$$\frac{H(X^{N+1})}{N+1} \leq \frac{H(X^N)}{N}$$

teda postupnosť  $H_N(X)$  je nerastúca. Keďže je ohraničená zdola nulou, má konečnú limitu.

Ďalej ukážeme, že táto limita sa rovná  $H(X/X^\infty)$ .

Platí

$$\begin{aligned} H_N(X) &= \frac{1}{N} \sum_{i=1}^N H(X_i/X^{i-1}) = \frac{1}{N} \sum_{i=1}^k H(X_i/X^{i-1}) + \\ &+ \frac{1}{N} \sum_{i=k+1}^n H(X_i/X^{i-1}) \leq \frac{k}{N} H(X) + \frac{N-k}{N} H(X_{k+1}/X^k) \end{aligned} \quad (2)$$

Nech  $\varepsilon > 0$  je ľubovoľne malé číslo. Zvolíme  $k$  tak, že

$$H(X_{k+1}/X^k) - H(X/X^\infty) \leq \frac{\varepsilon}{2} \quad (3)$$

k zvolenému  $k$  vyberieme  $N_0$  tak, že pri  $N > N_0$

$$\frac{kH(X)}{N} \leq \frac{\varepsilon}{2} \quad (4)$$

Potom pri  $N > N_0$  dostávame z nerovností (2), (3), (4)

$$H_N(X) \leq H(X/X^\infty) + \varepsilon$$



Na druhej strane

$$H_N(X) = \frac{1}{N} \sum_{i=1}^N H(X_i/X^{i-1}) \geq H(X_N/X^{N-1}) \geq H(X/X^\infty)$$

Pretože  $\varepsilon > 0$  je ľubovoľne malé, z týchto nerovností vyplýva, že postupnosť  $H_N(X)$ ,  $N = 1, 2, \dots$  konverguje k hodnote  $H(X/X^\infty)$ . Z uvedeného dôkazu vety vyplýva, že výdatnosť zdroja informácie nerastie s rastúcim  $N$ . To znamená, že ak zdroj vygeneruje v jednom symbole strednú informáciu  $H(X)$  a zdroj  $(X^N, P)$  v jednej  $N$ -tici strednú informáciu  $H(X^N)$ , potom z rovnosti

$$H(X^N) = nH(X)$$

vyplýva nerovnosť

$$N \leq n$$

t.j. pri kódovaní  $N$ -tíc symbolov je potrebná menšia, nanajvýš rovnaká dĺžka kódu než pri kódovaní symbolov jednotlivo, nezávisle na predchádzajúcich symboloch. Nevýhodou takéhoto kódovania je, že na prijímacej strane musíme dekódovať naraz celú  $N$ -ticu.

Ak by sme dekodovali po menších blokoch, môže sa stať, že niektoré bloky nie sú jednoznačne dekódovateľné. Rozdelíme preto množinu  $X^N$  na disjunktné množiny  $T_N, \bar{T}_N$ , kde

$T_N$  - množina jednoznačne dekódovateľných slov

$\bar{T}_N$  - množina viacznačne dekódovateľných slov.

Pravdepodobnosť chyby dekódovania je definovaná vzťahom

$$p_e = P(x \in \bar{T}_N)$$

Nech  $T_N$  je množina správ (blokov dĺžky  $N$ ) zdroja informácie, ktorú kódujeme rôznymi znakmi  $D$ -nárneho kódu abecedou  $U = \{u_1, u_2, \dots, u_L\}$ , kde všetky znaky majú rovnakú dĺžku

$$m = \frac{\log L}{\log D}$$

(dĺžka vyplýva z podmienky  $D^m = L$ ).

Definícia:

Dvojicu  $(U, T_N)$ , kde  $U, T_N$  sú vyššie uvedené voláme rovnomerným kódom zdroja. Veličinu

$$R = \frac{\log_2 L}{N} \quad [\text{Sh/symbol}]$$

kde  $L$  je kapacita kódu (počet znakov),  $N$  - dĺžka kódovaných postupností voláme rýchlosťou kódu zdroja ( $U, T_N$ ).

Ak kód zdroja je binárny, potom rýchlosť kódu zdroja udáva počet binárnych symbolov, ktoré sú potrebné na zakódovanie jedného symbolu zdroja. Pre nebinárne kódy je počet potrebných symbolov kódu

$$m = N \frac{R}{\log_2 D}$$

Pretože počet prvkov v množine  $T_N$  nie je väčší než  $M^N$ , platí

$$0 \leq R \leq \log M$$

Ak  $R = \log M$ , potom počet kódových slov sa rovná počtu postupností v množine  $X^N$ , t.j. všetky postupnosti môžu byť jednoznačne dekódovateľné.

Množinu  $X^N$  s  $M^N = 2^{N \log M}$  prvkami sme rozdelili na disjunktné podmnožiny  $T_N$  a  $\bar{T}_N$ , kde množina  $T_N$  obsahuje  $2^{NR}$  prvkov a množina  $\bar{T}_N$  obsahuje zvyšné prvky.

Z uvedeného vyplýva, že vlastnosti kódu zdroja nezávisia od voľby symbolov kódu ale len od rýchlosti kódu a množiny  $T_N$ . Preto kód zdroja budeme označovať  $(R, T_N)$ . Veličiny  $R$  a  $N$  udávajú kapacitu kódu  $L = 2^{NR}$  a  $T_N$  udáva množinu postupností symbolov dĺžky  $N$ , ktoré sú jednoznačne dekódovateľné.

Poznámka: Všetky dĺžky, ktoré z uvedených vzťahov vychádzajú neceločíselné, chápeme ako najmenšie celé číslo, ktoré nie je menšie než vypočítaná neceločíselná hodnota.

Ukážeme si ďalej niektoré vlastnosti stacionárneho zdroja bez pamäte, ktorý generuje symboly z  $\{X, p(x)\}$ . Pravdepodobnosť vygenerovania symbolu  $x \in X^N$  bude

$$p(x) = p(x_1, x_2, \dots, x_N) = \prod_{i=1}^N p(x_i)$$

Veta:

Nech  $T_N(\epsilon) \subseteq X^N$  je množina takých  $x \in T_N(\epsilon)$ , že

$$N[H(X) - \epsilon] \leq \sum_{x \in T_N(\epsilon)} p(x) \leq N[H(X) + \epsilon]$$

kde  $H(X)$  je entropia  $\{X, p(x)\}$ . Potom pre ľubovoľné malé kladné čísla  $\epsilon$ ,  $\delta$  existuje také  $n$ , že pre  $N > n$

$$p(T_N(\epsilon)) = \sum_{x \in T_N(\epsilon)} p(x) \geq 1 - \delta \quad (5)$$

$$(1 - \delta') 2^N [H(X) - \varepsilon] \leq M_\varepsilon \leq 2^N [H(X) + \varepsilon] \quad (6)$$

kde  $M_\varepsilon$  je počet postupností v množine  $T_N(\varepsilon)$ .

Dôkaz:

Pre stacionárny zdroj bez pamäti platí

$$J(\mathbf{x}) = \sum_{i=1}^N \log \frac{1}{p(x_i)} = \sum_{i=1}^N J(x_i)$$

kde  $J(x_i)$ ,  $i = 1, 2, \dots, N$  je postupnosť nezávislých náhodných veličín s rovnakým rozdelením. Aplikovaním zákona veľkých čísel na túto postupnosť dostávame, že pre ľubovoľné  $\varepsilon > 0$ ,  $\delta' > 0$  existuje také  $n$ , že pre  $N > n$  platí

$$p \left( \left| \frac{1}{N} \sum_{i=1}^N J(x_i) - H(X) \right| > \varepsilon \right) \leq \delta'$$

alebo

$$p \left( \left| \frac{1}{N} \sum_{i=1}^N J(x_i) - H(X) \right| \leq \varepsilon \right) \geq 1 - \delta'$$

Odtiaľ vyplýva (5). Z predpokladu vety dostávame

$$2^{-N} [H(X) - \varepsilon] \geq p(\mathbf{x}) \geq 2^{-N} [H(X) + \varepsilon]$$

Nech  $M_\varepsilon$  je počet prvkov množiny  $T_N(\varepsilon)$ . Platí

$$1 \geq \sum_{\mathbf{x} \in T_N(\varepsilon)} p(\mathbf{x}) \geq M_\varepsilon 2^{-N} [H(X) + \varepsilon]$$

Vyjadrením  $M_\varepsilon$  dostávame pravú časť nerovnosti (6).  
Z nerovnic

$$(1 - \delta') \leq \sum_{\mathbf{x} \in T_N(\varepsilon)} p(\mathbf{x}) \leq M_\varepsilon 2^{-N} [H(X) - \varepsilon]$$

dostaneme ľavú nerovnosť (6).

Veta (priama veta o kódovaní zdroja bez pamäti)

Pre každý stacionárny zdroj bez pamäti s abecedou  $X$  existuje pri  $R > H(X)$  taká postupnosť kódov

$$\{(R, T_N), N = 1, 2, \dots\}$$

že platí

$$\lim_{N \rightarrow \infty} P_e(R, T_N) = 0$$

Dôkaz:

Nech  $R > H(X)$  a  $\epsilon = R - H(X) > 0$ . Pre každé  $N$  zostrojíme  $(R, T_N)$  kód, pre ktorý  $T_N = T_N(\epsilon)$ . Potom podľa (5) platí uvedená veta.

Veta (obrátená veta o kódovaní zdroja bez pamäte)

Pre každý stacionárny zdroj bez pamäti s abecedou  $X$  existuje pri  $R < H(X)$  také číslo  $\delta > 0$ , že pre každé  $N$  a každý kód  $(R, T_N)$  je

$$P_e(R, T_N) > \delta$$

Okrem toho pre každú postupnosť kódov  $(R, T_N)$ ,  $N = 1, 2, \dots$  platí

$$\lim_{N \rightarrow \infty} P_e(R, T_N) = 1$$

Dôkaz neuvádzame, čitateľ ho môže nájsť v [10]. V tejto literatúre je aj návod dôkazu, že priama a inverzná veta o kódovaní stacionárneho zdroja platí aj všeobecnejšie - pre ergodické zdroje informácie, ak entropiu  $H(X)$  nahradíme entropiou  $H(X/X^\infty)$ .

Poznámka: Diskrétny stacionárny zdroj voláme ergodickým, ak pre ľubovoľné  $k$ , ľubovoľnú reálnu funkciu  $\psi(x_1, \dots, x_k)$ ,  $x_i \in X$ ,  $i = 1, 2, \dots, k$  a ľubovoľné kladné čísla  $\epsilon, \delta$  existuje také  $n$ , že pre všetky  $N > n$  platí

$$P \left( \left| \frac{1}{N} \sum_{i=1}^N \psi(x_1, \dots, x_k) - E[\psi(x)] \right| > \epsilon \right) \leq \delta$$

## 8.5 KANÁL PRENOSU INFORMÁCIE

Nech je daná vstupná abeceda kanála

$$X = \{x_1, x_2, \dots, x_{M_X}\}$$

výstupná abeceda kanála

$$Y = \{y_1, y_2, \dots, y_{M_Y}\}$$

vzdialenosť

$$d(\mathbf{x}, \mathbf{y}) \geq 0, \quad \mathbf{x} \in X^N, \quad \mathbf{y} \in Y^N$$