



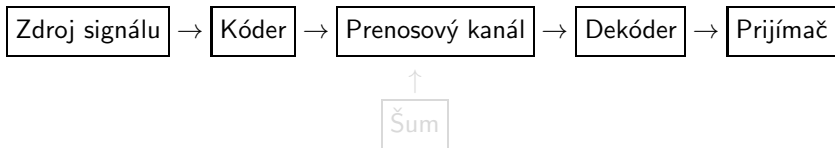
Prenosový kanál a jeho kapacita

Stanislav Palúch

Fakulta riadenia a informatiky, Žilinská univerzita

5. mája 2011

Prenosový reťazec



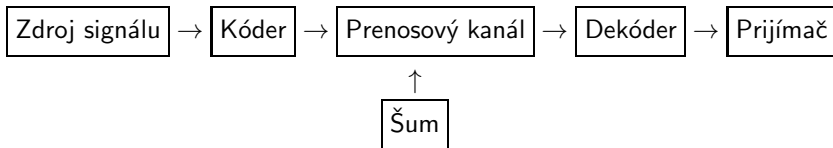
Prenosový kanál

- Prenosový kanál – komunikačné zariadenie so vstupom a výstupom.
- Vstup dokáže spracovávať znaky vstupnej abecedy Y .
- Z výstupu kanála vystupujú znaky výstupnej abecedy Z .

$$y_1, y_2, y_3, \dots \rightarrow \text{Prenosový kanál} \rightarrow z_1, z_2, z_3, \dots$$

- Vo väčšine prípadov $Y = Z$.

Prenosový reťazec



Prenosový kanál

- Prenosový kanál – komunikačné zariadenie so vstupom a výstupom.
- Vstup dokáže spracovávať znaky vstupnej abecedy Y .
- Z výstupu kanála vystupujú znaky výstupnej abecedy Z .

$$y_1, y_2, y_3, \dots \rightarrow \boxed{\text{Prenosový kanál}} \rightarrow z_1, z_2, z_3, \dots$$

- Vo väčšine prípadov $Y = Z$.

Príklad

Vstupná abeceda $Y = \{0, 1\}$ reprezentovaná napäťovými úrovňami

0 = L – (Low – nízka – napr. 0.7 V)

1 = H – (High – vysoká – napr. 5.5 V)

Výstupná abeceda $Z = \{0, 1, *\}$

0 – $\langle 0.7, 2.3 \rangle$

1 – $\langle 3.9, 5.5 \rangle$

* – $\langle 3.9, 5.5 \rangle$ – chyba

Príklad

Nech vstupnú abecedu Y kanála tvorí množina všetkých 8-bitových čísel s párnou paritou.

Ak ide o poruchový kanál, môžu sa na výstupe objaviť aj 8-bitové čísla s nepárnou paritou.

Výstupnou abecedou Z kanála je množina všetkých 8-bitových čísel.

Bezporuchový kanál

Definícia

Bezporuchový kanál je taký kanál, pri ktorom znak z_i prijatý v čase i jednoznačne závisí len od vyslaného slova $y_1, y_2, \dots, y_i - t. j.$

$$z_i = F_i(y_1, y_2, \dots, y_i) .$$

Ak znak z_i prijatý v čase i závisí len na vyslanom znaku $y_i - t. j.$

$$z_i = f_i(y_i) ,$$

potom hovoríme, že sa jedná o **prenosový kanál bez pamäte**.
Inak hovoríme, že ide o **prenosový kanál s pamäťou**.

Bezporuchový kanál teda jednoznačne popíšeme súborom funkcií $\{f_i\}_{i=1,2,\dots}$ resp. $\{F_i\}_{i=1,2,\dots}$.

Veľmi často f_i resp. F_i nezávisia na i a dokonca f_i býva identita.

Ak vyšleme cez rušený kanál vstupné slovo y_1, y_2, \dots, y_i , môžeme vplyvom porúch prijať ľubovoľné výstupné slovo z_1, z_2, \dots, z_i , pravda, s rôznou pravdepodobnosťou.

Podmienená pravdepodobnosť prijatia slova z_1, z_2, \dots, z_i za predpokladu, že bolo vyslané slovo y_1, y_2, \dots, y_i

$$\nu(z_1, z_2, \dots, z_i | y_1, y_2, \dots, y_i)$$

Definícia

Prenosový kanál \mathcal{C} je usporiadaná trojica $\mathcal{C} = (Y, Z, \nu)$, kde Y je vstupná abeceda, Z je výstupná abeceda a $\nu : \bigcup_{i=1}^{\infty} (Z^i \times Y^i) \rightarrow \langle 0, 1 \rangle$, pričom $\nu(z_1, z_2, \dots, z_i | y_1, y_2, \dots, y_i)$ je podmienená pravdepodobnosť, že na výstupe sa objaví slovo z_1, z_2, \dots, z_i za predpokladu, že na vstupe bolo slovo y_1, y_2, \dots, y_i .

$\nu_i(z_i|y_1, y_2, \dots, y_i)$ – podmienená pravdepodobnosť javu, že sa v čase i objaví na výstupe znak z_i za predpokladu, že na vstupe bolo slovo y_1, y_2, \dots, y_i . Potom

$$\nu_i(z_i|y_1, y_2, \dots, y_i) = \sum_{z_1, z_2, \dots, z_{i-1}} \nu(z_1, z_2, \dots, z_i|y_1, y_2, \dots, y_i).$$

Hovoríme, že kanál \mathcal{C} je **kanál bez pamäte**, ak $\nu_i(z_i|y_1, y_2, \dots, y_i)$ závisí iba na y_i , t. j. ak

$$\nu_i(z_i|y_1, y_2, \dots, y_i) = \nu_i(z_i|y_i).$$

Ak navyše $\nu_i(z_i|y_i)$ nezávisí na i , t. j. ak $\nu_i(z_i|y_i) = \nu(z_i|y_i)$, hovoríme, že \mathcal{C} je **stacionárny kanál bez pamäte**.

Ak

$$\nu(z_1, z_2, \dots, z_i|y_1, y_2, \dots, y_i) = \nu(z_1|y_1)\nu(z_2|y_2) \dots \nu(z_i|y_i) = \prod_{k=1}^i \nu(z_k|y_k),$$

hovoríme, že \mathcal{C} je **stacionárny nezávislý kanál**.

$\nu_i(z_i|y_1, y_2, \dots, y_i)$ – podmienená pravdepodobnosť javu, že sa v čase i objaví na výstupe znak z_i za predpokladu, že na vstupe bolo slovo y_1, y_2, \dots, y_i . Potom

$$\nu_i(z_i|y_1, y_2, \dots, y_i) = \sum_{z_1, z_2, \dots, z_{i-1}} \nu(z_1, z_2, \dots, z_i|y_1, y_2, \dots, y_i).$$

Hovoríme, že kanál \mathcal{C} je **kanál bez pamäte**, ak $\nu_i(z_i|y_1, y_2, \dots, y_i)$ závisí iba na y_i , t. j. ak

$$\nu_i(z_i|y_1, y_2, \dots, y_i) = \nu_i(z_i|y_i).$$

Ak navyše $\nu_i(z_i|y_i)$ nezávisí na i , t. j. ak $\nu_i(z_i|y_i) = \nu(z_i|y_i)$, hovoríme, že \mathcal{C} je **stacionárny kanál bez pamäte**.

Ak

$$\nu(z_1, z_2, \dots, z_i|y_1, y_2, \dots, y_i) = \nu(z_1|y_1)\nu(z_2|y_2)\dots\nu(z_i|y_i) = \prod_{k=1}^i \nu(z_k|y_k),$$

hovoríme, že \mathcal{C} je **stacionárny nezávislý kanál**.

$\nu_i(z_i|y_1, y_2, \dots, y_i)$ – podmienená pravdepodobnosť javu, že sa v čase i objaví na výstupe znak z_i za predpokladu, že na vstupe bolo slovo y_1, y_2, \dots, y_i . Potom

$$\nu_i(z_i|y_1, y_2, \dots, y_i) = \sum_{z_1, z_2, \dots, z_{i-1}} \nu(z_1, z_2, \dots, z_i|y_1, y_2, \dots, y_i).$$

Hovoríme, že kanál \mathcal{C} je **kanál bez pamäte**, ak $\nu_i(z_i|y_1, y_2, \dots, y_i)$ závisí iba na y_i , t. j. ak

$$\nu_i(z_i|y_1, y_2, \dots, y_i) = \nu_i(z_i|y_i).$$

Ak navyše $\nu_i(z_i|y_i)$ nezávisí na i , t. j. ak $\nu_i(z_i|y_i) = \nu(z_i|y_i)$, hovoríme, že \mathcal{C} je **stacionárny kanál bez pamäte**.

Ak

$$\nu(z_1, z_2, \dots, z_i|y_1, y_2, \dots, y_i) = \nu(z_1|y_1)\nu(z_2|y_2)\dots\nu(z_i|y_i) = \prod_{k=1}^i \nu(z_k|y_k),$$

hovoríme, že \mathcal{C} je **stacionárny nezávislý kanál**.

$\nu_i(z_i|y_1, y_2, \dots, y_i)$ – podmienená pravdepodobnosť javu, že sa v čase i objaví na výstupe znak z_i za predpokladu, že na vstupe bolo slovo y_1, y_2, \dots, y_i . Potom

$$\nu_i(z_i|y_1, y_2, \dots, y_i) = \sum_{z_1, z_2, \dots, z_{i-1}} \nu(z_1, z_2, \dots, z_i|y_1, y_2, \dots, y_i).$$

Hovoríme, že kanál \mathcal{C} je **kanál bez pamäte**, ak $\nu_i(z_i|y_1, y_2, \dots, y_i)$ závisí iba na y_i , t. j. ak

$$\nu_i(z_i|y_1, y_2, \dots, y_i) = \nu_i(z_i|y_i).$$

Ak navyše $\nu_i(z_i|y_i)$ nezávisí na i , t. j. ak $\nu_i(z_i|y_i) = \nu(z_i|y_i)$, hovoríme, že \mathcal{C} je **stacionárny kanál bez pamäte**.

Ak

$$\nu(z_1, z_2, \dots, z_i|y_1, y_2, \dots, y_i) = \nu(z_1|y_1)\nu(z_2|y_2)\dots\nu(z_i|y_i) = \prod_{k=1}^i \nu(z_k|y_k),$$

hovoríme, že \mathcal{C} je **stacionárny nezávislý kanál**.

Stacionárny nezávislý kanál

Majme stacionárny nezávislý kanál so vstupnou abecedou $A = \{a_1, a_2, \dots, a_n\}$ a výstupnou abecedou $B = \{b_1, b_2, \dots, b_r\}$.

Označme $q_{ij} = \nu(b_j|a_i)$ pravdepodobnosť, že ak je na vstupe kanála vstupný znak a_i , na výstupe sa objaví znak b_j .

Hodnoty q_{ij} sa volajú **prenosové pravdepodobnosti** a matica typu $n \times r$

$$\mathbf{Q} = \begin{pmatrix} q_{11} & q_{12} & \dots & q_{1r} \\ q_{21} & q_{22} & \dots & q_{2r} \\ \dots & \dots & \dots & \dots \\ q_{n1} & q_{n2} & \dots & q_{nr} \end{pmatrix}$$

je **matica prenosových pravdepodobností**.

Poznámka

Súčet prvkov každého riadku matice \mathbf{Q} sa rovná 1, t. j. $\sum_{j=1}^r q_{kj} = 1$ pre každé $k = 1, 2, \dots, n$.

- $P(a_i) = p_i$ – pravdepodobnosť javu, že sa na vstupe kanála objaví znak a_i .
- $P(a_i \cap b_j)$ – pravdepodobnosť javu že na vstupe kanála bude znak a_i a na jeho výstupe znak b_j ,
- $P(b_j)$ – pravdepodobnosť , že sa na výstupe kanála objaví b_j
- $q_{ij} = \nu(b_j|a_i)$ pravdepodobnosť, že ak je na vstupe kanála vstupný znak a_i , na výstupe sa objaví znak b_j .

$$P(a_i \cap b_j) = p_i q_{ij}.$$

$$P(b_j) = P(a_1 \cap b_j) + P(a_2 \cap b_j) + \dots + P(a_n \cap b_j) = \sum_{t=1}^n p_t q_{tj}.$$

Stacionárny nezávislý kanál

- Na výskyt znaku a_i na vstupe kanála resp. znaku b_j na výstupe kanála sa môžeme pozerať ako na výsledky pokusov

$$\mathbf{A} = \{\{a_1\}, \{a_2\}, \dots, \{a_n\}\},$$

$$\mathbf{B} = \{\{b_1\}, \{b_2\}, \dots, \{b_r\}\}.$$

Príjemcu správ na výstupe kanála zaujíma, aký znak bol vyslaný – teda aký bol výsledok pokusu \mathbf{A} .

Má však k dispozícii len výsledok pokusu \mathbf{B} .

Stredná hodnota informácie obsiahnutá v pokuse \mathbf{B} o pokuse \mathbf{A} sa dá vyjadriť ako spoločná informácia $I(\mathbf{A}, \mathbf{B})$ pokusov \mathbf{A} , \mathbf{B} , pre ktorú využijeme vzťah

$$I(\mathbf{A}, \mathbf{B}) = \sum_{i=1}^n \sum_{j=1}^r P(A_i \cap B_j) \cdot \log_2 \left(\frac{P(A_i \cap B_j)}{P(A_i) \cdot P(B_j)} \right).$$

$$I(\mathbf{A}, \mathbf{B}) = \sum_{i=1}^n \sum_{j=1}^r P(a_i \cap b_j) \log_2 \frac{P(a_i \cap b_j)}{P(a_i)P(b_j)}$$

$$\begin{aligned}P(a_i) &= p_i \\P(a_i \cap b_j) &= p_i q_{ij} \\P(b_j) &= \sum_{t=1}^n p_t q_{tj}\end{aligned}$$

$$\begin{aligned}I(\mathbf{A}, \mathbf{B}) &= \sum_{i=1}^n \sum_{j=1}^r P(a_i \cap b_j) \log_2 \frac{P(a_i \cap b_j)}{P(a_i)P(b_j)} \\&= \sum_{i=1}^n \sum_{j=1}^r p_i q_{ij} \log_2 \frac{p_i q_{ij}}{p_i \sum_{t=1}^n p_t q_{tj}} \\&= \sum_{i=1}^n p_i \sum_{j=1}^r q_{ij} \log_2 \frac{q_{ij}}{\sum_{t=1}^n p_t q_{tj}}.\end{aligned}\tag{1}$$

Ak sa bude pokus \mathbf{A} mnohokrát nezávisle opakovať, výraz (1) je stredné množstvo informácie prenesené kanálom pripadajúce na jeden znak.

Maximalizácia množstva prenesenej informácie

Množstvo prenesenej informácie $I(\mathbf{A}, \mathbf{B})$ je funkciou pravdepodobností

$p_1, p_2, \dots, p_n,$

$$I(\mathbf{A}, \mathbf{B}) = I(\mathbf{A}, \mathbf{B})(p_1, p_2, \dots, p_n) = \sum_{i=1}^n p_i \sum_{j=1}^r q_{ij} \log_2 \frac{q_{ij}}{\sum_{t=1}^n p_t q_{tj}}.$$

Maximalizovať množstvo prenesenej informácie – hľadať viazaný extrém funkcie F za podmienky $\sum_{i=1}^n p_i, p_i \geq 0$ pre $i = 1, 2, \dots, n$.

Položme

$$\begin{aligned} F(p_1, p_2, \dots, p_n) &= I(A, B) + \lambda \left(1 - \sum_{i=1}^n p_i \right) = \\ &= \sum_{i=1}^n p_i \sum_{j=1}^r q_{ij} \underbrace{\log_2 \frac{q_{ij}}{\sum_{t=1}^n p_t q_{tj}}}_{(*)} + \lambda \left(1 - \sum_{i=1}^n p_i \right). \quad (2) \end{aligned}$$

Parciálna derivácia výrazu (*) v (2) sa vypočíta takto:

$$\begin{aligned} \frac{\partial}{\partial p_k} \log_2 \frac{q_{ij}}{\sum_{t=1}^n p_t q_{tj}} &= \frac{\partial}{\partial p_k} \log_2(e) \cdot \ln \frac{q_{ij}}{\sum_{t=1}^n p_t q_{tj}} = \\ &= \log_2(e) \cdot \frac{\sum_{t=1}^n p_t q_{tj}}{q_{ij}} \cdot \frac{q_{ij}}{-\left(\sum_{t=1}^n p_t q_{tj}\right)^2} \cdot q_{kj} = -\log_2(e) \cdot \frac{q_{kj}}{\sum_{t=1}^n p_t q_{tj}}. \end{aligned}$$

$$\frac{\partial F}{\partial p_k} = \sum_{j=1}^r q_{kj} \log_2 \frac{q_{kj}}{\sum_{t=1}^n p_t q_{tj}} - \underbrace{(\log_2 e + \lambda)}_{\gamma}.$$

Položením parciálnych derivácií nule, dostaneme nasledujúcu sústavu rovníc pre neznáme p_1, p_2, \dots, p_n a γ :

$$\sum_{i=1}^n p_i = 1 \quad (3)$$

$$\sum_{j=1}^r q_{kj} \log_2 \frac{q_{kj}}{\sum_{t=1}^n p_t q_{tj}} = \gamma \quad \text{pre } k = 1, 2, \dots, n. \quad (4)$$

Dá sa ukázať, že funkcia $I(\mathbf{A}, \mathbf{B})$ (1) je konkávna, a že splnenie podmienok (3) a (4) stačí na to, aby príslušná hodnota funkcie $I(\mathbf{A}, \mathbf{B})$ bola maximálna.

Rovnice (3) a (4) nazveme **kapacitné rovnice kanála**.



Množstvo prenesenej informácie

Pripojme na vstup kanála zdroj $\bar{\mathcal{S}} = (Y^*, \mu)$.

Pravdepodobnosť vyslania slova $\mathbf{y} = (y_1, y_2, \dots, y_n)$ je $\mu(y_1, y_2, \dots, y_n)$.

Ak sa na vstupe kanála $\mathcal{C} = (Y, Z, \nu)$ budú objavovať vstupné slova zo zdroja $\bar{\mathcal{S}}$, jeho výstup sa bude javiť ako zdroj označovaný symbolom

$$\mathcal{R} = \mathcal{R}(\mathcal{C}, \bar{\mathcal{S}})$$

s abecedou Z a pravdepodobnostnou funkciou π , pre ktorú platí

$$\begin{aligned} \pi(\mathbf{z}) &= \pi(z_1, z_2, \dots, z_n) = \\ &= \sum_{\mathbf{y} \in Y^n} \nu(\mathbf{z}|\mathbf{y})\mu(\mathbf{y}) = \sum_{y_1 y_2 \dots y_n \in Y^n} \nu(z_1, z_2, \dots, z_n | y_1, y_2, \dots, y_n) \cdot \mu(y_1, y_2, \dots, y_n). \end{aligned}$$

Pripojme na vstup kanála zdroj $\bar{S} = (Y^*, \mu)$.

Pravdepodobnosť vyslania slova $\mathbf{y} = (y_1, y_2, \dots, y_n)$ je $\mu(y_1, y_2, \dots, y_n)$.

Ak sa na vstupe kanála $C = (Y, Z, \nu)$ budú objavovať vstupné slova zo zdroja \bar{S} , jeho výstup sa bude javiť ako zdroj označovaný symbolom

$$\mathcal{R} = \mathcal{R}(C, \bar{S})$$

s abecedou Z a pravdepodobnostnou funkciou π , pre ktorú platí

$$\begin{aligned} \pi(\mathbf{z}) &= \pi(z_1, z_2, \dots, z_n) = \\ &= \sum_{\mathbf{y} \in Y^n} \nu(\mathbf{z}|\mathbf{y})\mu(\mathbf{y}) = \sum_{y_1 y_2 \dots y_n \in Y^n} \nu(z_1, z_2, \dots, z_n | y_1, y_2, \dots, y_n) \cdot \mu(y_1, y_2, \dots, y_n). \end{aligned}$$

Okrem výstupného zdroja $\mathcal{R} = \mathcal{R}(\mathcal{C}, \bar{\mathcal{S}})$ môžeme dvojici vstupného zdroja $\bar{\mathcal{S}}$ a kanála \mathcal{C} priradiť ešte aj tzv. dvojitého zdroj $\mathcal{D} = ((Y \times Z)^*, \psi)$, ktorý akoby vysielal dvojice (y_i, z_i) vstupného a výstupného znaku. Ak stotožníme slovo $(y_1, z_1)(y_2, z_2) \dots (y_n, z_n)$ s usporiadanou dvojicou

$$(\mathbf{y}, \mathbf{z}) = ((y_1, y_2, \dots, y_n), (z_1, z_2, \dots, z_n)),$$

môžeme pravdepodobnosť $\psi(\mathbf{y}, \mathbf{z})$ vypočítať nasledovne

$$\psi(\mathbf{y}, \mathbf{z}) = \nu(\mathbf{z}|\mathbf{y}) \cdot \mu(\mathbf{y}) .$$

Množstvo prenesenej informácie

Fixujme n a označme $\mathbf{A}_n, \mathbf{B}_n$ rozklady množiny $Y^n \times Z^n$, na množiny tvaru

$$\mathbf{B}_n = \{ \{Y^n \times \mathbf{z}\} \mid \mathbf{z} \in Z^n \} = \{ Y^n \times \{(z_1, \dots, z_n)\} \mid (z_1, \dots, z_n) \in Z^n \}$$

$$\mathbf{A}_n = \{ \{\mathbf{y} \times Z^n\} \mid \mathbf{y} \in Y^n \} = \{ \{(y_1, \dots, y_n)\} \times Z^n \mid (y_1, \dots, y_n) \in Y^n \}$$

Definujme ešte kombinovaný pokus $\mathbf{D}_n = \mathbf{A}_n \wedge \mathbf{B}_n$. Podľa definície je

$$\mathbf{D}_n = \{ (\mathbf{y}, \mathbf{z}) \mid \mathbf{y} \in Y^n, \mathbf{z} \in Z^n \}$$

Odpoveď na výsledok pokusu \mathbf{A}_n nám hovorí, aké slovo bolo vyslané. To ale na prijímacej strane kanála \mathcal{C} nevieme.

Vieme však výsledok pokusu \mathbf{B}_n .

Stredná hodnota informácie o pokuse \mathbf{A}_n v pokuse \mathbf{B}_n je $I(\mathbf{A}_n, \mathbf{B}_n)$.

Na jeden znak pripadá

$$\frac{1}{n} \cdot I(\mathbf{A}_n, \mathbf{B}_n)$$

a pre veľmi dlhé správy

$$I(\bar{\mathcal{S}}, \mathcal{R}) = \lim_{n \rightarrow \infty} \frac{1}{n} \cdot I(\mathbf{A}_n, \mathbf{B}_n)$$

Vieme, že pre entropie vstupného zdroja $\bar{\mathcal{S}}$, výstupného zdroja $\mathcal{R}(\mathcal{C}, \bar{\mathcal{S}})$ a dvojitého zdroja $\bar{\mathcal{D}}$ platí

$$H(\bar{\mathcal{S}}) = \lim_{n \rightarrow \infty} \frac{1}{n} \cdot H(\mathbf{B}_n)$$

$$H(\mathcal{R}) = \lim_{n \rightarrow \infty} \frac{1}{n} \cdot H(\mathbf{A}_n)$$

$$H(\mathcal{D}) = \lim_{n \rightarrow \infty} \frac{1}{n} \cdot H(\mathbf{D}_n)$$

$$I(\mathbf{A}_n, \mathbf{B}_n) = H(\mathbf{A}_n) + H(\mathbf{B}_n) - H(\mathbf{D}_n)$$

$$I(\bar{\mathcal{S}}, \mathcal{R}) = \lim_{n \rightarrow \infty} \frac{1}{n} \cdot I(\mathbf{A}_n, \mathbf{B}_n) = H(\bar{\mathcal{S}}) + H(\mathcal{R}) - H(\mathcal{D}).$$

Kapacitu kanála môžeme definovať troma spôsobmi

- pomocou maximálneho množstva informácie pripadajúcej na jeden znak, ktoré je kanál schopný preniesť – $C_1(\mathcal{C})$
- pomocou maximálnej entropie zdroja, ktorého správy je kanál schopný prenášať s ľubovoľne malým rizikom – $C_2(\mathcal{C})$
- pomocou počtu spoľahlivo prenesených postupností – $C_3(\mathcal{C})$.

Kapacita kanála prvého druhu

Kapacitu prvého druhu definujeme nasledovne

$$C_1(\mathcal{C}) = \sup_{\bar{\mathcal{S}}} I(\bar{\mathcal{S}}, \mathcal{R}(\mathcal{C}, \bar{\mathcal{S}})),$$

kde suprémum berieme cez množinu všetkých zdrojov s abecedou Y .
Ostatné kapacity nešpecifikujeme, platí však $C_1(\mathcal{C}) = C_1(\mathcal{C}) = C_1(\mathcal{C})$.

Veta (Priama Shannonova veta)

Ak pre stacionárny nezávislý zdroj S a pre stacionárny nezávislý kanál C platí

$$H(S) < C(C),$$

potom možno správy zdroja S preniesť cez kanál C s ľubovoľne malým rizikom.

Veta (Obrátená Shannonova veta)

Ak pre stacionárny nezávislý zdroj S a pre stacionárny nezávislý kanál C platí

$$H(S) > C(C),$$

potom nemožno správy zdroja S preniesť cez kanál C s ľubovoľne malým rizikom.